
الجرائم
المعلوماتية
في دولة الإمارات والوطن العربي

# الجرائم المعلوماتية

## في دولة الإمارات والوطن العربي

المستشار/ **أيـمـن رسـلان**

القـاضي بمحـاكـم دبـي

والمستشار بمحكمة الإستئناف العليا

بالقاهرة



# الجرائم المعلوماتية

## في دولة الإمارات والوطن العربي

**Cyber Crimes** in UAE and the Arab World

**أيمن رسلان**

**Ayman Reslan**

**الطبعة الأولى: أيلول/ سبتمبر 2016**

ISBN: 978 - 9948 - 02 - 684 - 6

موافقة «المجلس الوطني للإعلام»
بدولة الإمارات العربية المتحدة
رقم: (142499) تاريخ (21/ 08/ 2016)

لا يجوز نشر أي جزء من هذا الكتاب، أو نقله على أي نحو، وبأي طريقة، سواء أكانت إلكترونية أم ميكانيكية أم بالتصوير أم التسجيل أم خلاف ذلك، إلَّا بموافقة الناشر على ذلك كتابة مقدماً.

© **جميع حقوق النشر محفوظة للناشر 2016**



قنديل | Qindeel | للطباعة والنشر والتوزيع | Printing - Publishing & Distribution
ص. ب: 71474 شارع الشيخ زايد ـ دبي ـ دولة الإمارات العربية المتحدة
البريد الإلكتروني: info@qindeel.ae ـ الموقع الإلكتروني: www.qindeel.ae

# مقدمة

عندما شاع استخدام الحاسب الآلي في أنحاء العالم، بما فى ذلك مصر وغيرها من الدول العربية، أصبح العالم في مواجهة كيان جديد وغريب، غزا على نحو واسع وكبير جميع مناحي وشؤون حياتنا، وأخذ يتطور شيئاً فشيئاً بصورة مضطردة، ما جعله يؤدي مهامَّ ووظائـفَ، لا طاقة لآلاف البشر بها، بل بات واضحا أن هذا الجهاز مخزنٌ لمعلومات وأسرار الناس، بل وخطط أحلامهم ومستقبلهم، واحتل مكانة الحاكم والناظم لكل شيء؛ آلات المصانع والمعامل، حركة الطائرات، وعمل البنوك. . . إلخ.

وغنيّ عن البيان القول بأن المجتمع البشريّ بهذا الاختراع الجديد إنما صنع ثورة معلومات ضخمة. وما لبث الناس إلاّ قليلاً وهم يفيقون من صدمة هذه الثورة حتى هاجمتهم ثورة جديدة خلقها ذلك التزاوج، أو الاتحاد الفريد بين هذا الاختراع الجديد وأنظمة الاتصالات الحديثة، لنصل في نهاية القرن العشرين وأوائل القرن الحادي والعشرين إلى ما أُطلق عليه «التواصل عبر شبكة الإنترنت الدولية»، التي انهارت أمامها الحدود بين الدول وتلاشت المسافات بين الأفراد والجماعات.

وبالولوج، بعيداً عن الاستخدامات الطيبة والمفيدة للحاسب الآلي، ظهرت لنا أمور وضعت هذه المحاسن فى كفةٍ وفى الكفّة الأخرى مساوئ لا حَصْر لها ولا عَدّ، سواءٌ تعلقت بجرائم معلوماتية أو رقمية، أو السطو على بياناتِ ومعلوماتِ وأسرارِ الناس وفَضْحهم على شبكة المعلومات الدولية، فهي ـ أي الجرائم الرقمية ـ إما أن تقع على الكمبيوتر ذاته، وإما أن تقع بوساطته، حيث يصبح أداةً في يد الجاني يستخدمه لتحقيق أغراضه غير المشروعة.

وتأسيساً على هذا التطور السلبى فى هذا المجال شرع الكثيرُ من الدول فى تدشين تشريعات جنائية خاصة لمكافحة جرائم الكمبيوتر، التي تعتبر ظاهرة مستحدثة على علم الإجرام، وفي صدارة هذه الدول تأتي أمريكا وفرنسا ودول الاتحاد الأوروبي الأخرى.

هذا المسعى من جانب بعض الدول، إنما يرجع إلى أنّ العالم بات كقرية صغيرة، وانفردت قرية داخِلَها بالتميز والانفراد، وإعجاب جميع أصحاب المصالح المشروعة وغير المشروعة، هى قرية المعلوماتية والإنترنت، حيث بدأت تقنية المعلومات تفرز آثاراً شاملة على البنية الإدارية والاقتصادية والاجتماعية والسياسية، والثقافية،والقانونية للدول، ذلك أن كل اختراع علمي لابد أن يفتح آفاقاً جديدة ويرتب أثاراً لم تكن قائمة قبل وجوده وانتشاره. وهنا كان لا بدّ للقانون من أن يتدخل، ليحسم المسائل الخِلافية ويردع المجرمين والمخالفين في ظل هذا التداحل المعلوماتي شديد التعقيد.

ومن الأهمية بمكان القول إن جرائم الحاسب الآلي، هى ظاهرة إجرامية جديدة ومستجدّة، تقرع في جنباتها أجراسَ الخطر لتنبه مجتمعات العصر الراهن إلى حجم المخاطر وهول الخسائر الناجمة عن جرائم الحاسب الآلي، التي تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة. فهذه الجرائم، تنطوى على عمليات تقنية عالية لارتكاب الجريمة على نحو منظّم وغير قابل للاكتشاف. ذلك أن الجُناة هم من الذكاء والاحتراف ما يجعلهم ينالون

أغراضهم بكل سهولة ويُسْر سواءٌ كانت هذه الأغراض سطواً على الحق في المعلومات، أو تخريباً لقواعد بيانات أشخاص أو شركات، المهمّ أن يصل المجرم إلى غرضه سواءٌ كان نافعا له أو ضارّاً بغيره.

وينبغي أن نؤكد على أن هذه الدراسة جديرةٌ بالاعتبار، لأنها تتعلق بتحليل وتمحيص الثورة المعلوماتية التي نعيشها هذه الأيام، وإن كان تناولنا يركز بالأساس على الجانب السلبيّ من هذ الثورة، وهو جانب الجرائم الرقمية والمعلوماتية، ومدى تأثير ذلك على العالم واستقرار العلاقات فيه ودوامها.

ومما هو جدير بالملاحظة، أن وسائل الاتصال لم تخترع الجريمة، بل كانت ضحيةً لها في معظم الأحوال،. حيث أن هذه الوسائل تعرضت لسوء الاستغلال من قبل كثيرين، ومن الثابت أيضاً أن المجرمين وظّفوا الاتصال تاريخياً ـ ضمن أدواتهم على اختلافها ـ لخدمة النشاطات الإجرامية التي يقومون بها. أما الجريمة، فهي الجريمة ذاتها في قديم التاريخ، وحديثه، لا يختلف على بشاعتها وخطرها على المجتمع الإنساني أحد. ولذلك اتُّفق على مواجهتها، ومن أجلها أقيمت المحاكم، وسُنَّت العقوبات، تستوي في النظرة إليها ـ كسلوك شاذ ـ الشرائع السماوية كلُّها، والقوانين الوضعية كافةً.

وإزاء ذلك كلّه، كان لا بدّ من تكاتف الدول من أجل مكافحة هذا النوع المستحدث من الجرائم، التي لم تعد تتمركز في دولة معينة، ولا توجّه لمجتمع بعينه، بل أصبحت تعبر الحدود لتُلحِق الضرر بدول ومجتمعات عديدة، مستغلةً التطور الكبير للوسائل التقنية الحديثة في الاتصالات والمواصلات، وتعزيز التعاون فيما بينها، واتخاذ تدابير فعّالة للحدّ منها والقضاء عليها ومعاقبة مرتكبيها.

المؤلف

# الفصل الأول

# حول التعريف بجرائم المعلوماتية والإنترنت وتطورها

أرجعَ الفقه الجنائي جرائم الحاسوب إلى عام 1960. وأما جرائم الإنترنت فإنه يمكن القول إنها بدأت مع عام 1988، وكانت أول الجرائم التي ترتبط عضوياً بالإنترنت هي جرائم العدوان الڤيروسي، فيما هو معروف في التاريخ القانوني بجريمة دودة موريس المؤخرة واقعتها في 2 / نوفمبر/ تشرين الثاني 1988.

ولا يزال الفقه والتشريع المقارن، في حقيقة الأمر، يستشعران الحرج في التمييز بين كل من جرائم الحاسوب وبين تلك الناجمة عن استخدام الإنترنت، حتى إن تقرير الأمم المتحدة عن منع الجريمة عام 1995 تبنّى الموقف المقارن المذكور هذا فصدر عنوان التقرير Computer crimes & other crimes related to computer.

لذلك نجد أن تعريف جرائم الحاسوب في الفقه والتشريع، يسوده اتجاهٌ يجمع بين الجرائم التي تقع على الحاسوب ذاته، وتلك التي يكون الحاسوب وسيلة ارتكابها؛ فهي لدى هذا الاتجاه تعرف بأنها «فعلٌ غير مشروع يتورط نظام الحاسوب فيه، سواءٌ كان الحاسوب كآلةٍ هو موضوع الجريمة، أو كان الوسيلة

إلى ارتكابها، أو مستودع الدليل المرتبطِ بالجريمة». وهو تعريف مستمدّ من أكثر التعريفات شعبيةً لجرائم الحاسوب الذي قال فيه الأستاذ Donn Parker من حيث إن جرائم الحاسوب هي «جرائم تتطلب دراية ضرورية بالحاسوب لكي يتم ارتكاب الجريمة بنجاح». ولم تأت الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي المؤرخة 23/ 11/ 2001 على تعريف محدد للجريمة عبر الإنترنت، وإنما اعترفت بنوعية من الجرائم يمكن ارتكابها عبر الإنترنت.

ولقد توسّعت إدارة العدل الأمريكية في ربط الحاسوب بتقنيته، فذهبت إلى تعريف جرائم الحاسوب بأنها «هي كل عدوان بالارتكاب على أي قانون يتضمن في محتواه تقنية الحاسوب ويكون عرضةً للتحقيق والاتهام». كان ذلك بالطبع، بتأثير من اتجاهات المشرِّع الأمريكي في تعديل 1996 لقانون البنية الوطنية للمعلومات The National Infrastructure Information Act (القسم 1030)، الذي استُوحِيَ التجريم من الربط بين الحاسوب وتقنيته ككل، فتمخض هذا الاتجاه عن وجود ثلاثة أنواع من الجرائم التي يمكن ارتكابها عبر الحاسوب وذلك وفقاً للمنهج الأمريكي، وهي :

أولاً : الجرائم التي يكون الحاسوب هدفاً لها، وهي نوعية من الجرائم يكون هدف المجرم فيها التوصل إلى سرقة بيانات من الحاسوب أو إحداث إضرار به أو بنظام تشغيله أو بالشبكة التي يعمل من خلالها.

ثانياً : الجرائم التي يكون الحاسوب وسيلةً لارتكابها، وهذه النوعية من الجرائم تحدث عندما يستخدم المجرم الحاسوب لتسهيل ارتكاب بعض الجرائم التقليدية، مثل الاحتيال على البنوك؛ كما لو قام موظف في أحد البنوك باستخدام برمجية تحويل العملة لصالحه فيودع مبالغ مُحوّلة لحسابه عوضاً عن وضعها في مسارها الصحيح، وكذلك القيام بإعداد Produce أو نقل Transfer أو حيازة Possess آلة Device بما في ذلك الحاسوب بنيّة استخدامها في تزوير

وثائق إثبات شخصية To Falsify Identification documentation (18 USCode Sec. 1028).

ولقد توسّع بعض التشريعات في مدلول مصطلح «أدوات التزوير Forgery Devices» لكي تشمل الحاسوب وملحقاته Equipment وبرمجياته Software إذا أُعدّت خصيصاً بغرض التزوير، مثل قانون ولاية نيوجيرسي (N.J.Stat.ANN. Sec. 2 C: 21-1، N.J.Stat.ANN.Sec.2C:21-1).

ثالثاً: الجرائم التي يكون فيها الحاسوب أداةً لحفظ الأدلة دون أن يكون وسيطاً في الحصول عليها، كما هو الحال في قيام مروِّجي المخدرات والاتجار غير المشروع فيها، وكذلك مُعدّي البرمجيات المُعتَدى على حقوق الملكية فيها وكذلك السرقة الإلكترونية التي تتم عدواناً على حقوق المؤلف، بوضع سرقاتهم وملفاتهم وسجلاتهم في الحاسوب.

ومما تجدر الإشارة، إليه إن مثل هذا التقسيم السالف ليس جامعاً مانعاً للتعبير عن جرائم الحاسوب كافةً، إذ هناك من الجرائم التي ترتكب بواسطة الحاسوب، ومع ذلك لا يمكن إدراجها في أيٍّ من الأقسام أو الأشكال الثلاثة مثلما هو الحال في جريمة سرقة وقت الحاسوب مثلاً، وهي جريمة يعرفها القسم Tit. 18 USCode Sec. 641 من التقنين الأمريكي كجريمة من جرائم المعلوماتية.

وربما يكون السبب في التوسع السالف عائداً إلى أن إمكانيات الحاسوب لم تبرز إلى الوجود بالشكل الذي يجب أن تكون عليه، فكل ما نعلمه عن قدرات الحاسوب يقل كثيراً عما نعلمه عن قدرات الإنترنت. فهذه الأخيرة، وإن كانت لم تأخذ حظها كما ينبغي، فقد تناولها الساسة وفقهاء القانون والاقتصاد على المستوى الإقليمي والدولي بكثير من التأمل وهي بعد في بداياتها، في حين إن مسيرة الحاسوب تبدو هادئة أو طبيعية. ومثل هذا الأمر وُجِد له تأثير كبير في الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي المؤرخة 23/ 11/ 2001 حيث

اعترفت الاتفاقية، في المادة الأولى منها، بمصطلح «نظام الحاسوب Computer System» ولم تأخذ في الاعتبار مجرد مصطلح «الحاسوب Computer» فقد حددت الاتفاقية هذا المصطلح بكونه يشمل «أية آلة أو مجموعة مرتبطة فيما بينها أو ذات علاقة من الآلات، يمكن بإضافة برمجية إلى واحد أو أكثر منها، أن تقوم بمعالجة آلية للبيانات».

إننا إذن أمام مفارقة بين الحاسوب وبين أحد تقنياته. وهناك ما يميز الاثنين على الرغم من التعميم (الحاسوب) والتخصيص (الإنترنت). وهو تمييز يقوم على أكثر المظاهر بساطةً، إذ إنه لكي يتم لنا الولوج إلى الحاسوب فإن علينا فقط أن نضغط مفتاح تشغيله، أما الإنترنت فإننا نحتاج، فضلاً عن جهاز حاسوبٍ عاملٍ، إلى الولوج إليها بالاتصال بوسيط هو مزود الإنترنت Provider يمكننا من التعامل مع الخادم Surver، هو أمر يُحتاج إليه خصوصاً من خلال الحاسوب.

إن ذلك، في الحقيقة، يجعلنا نقف في تأمُّل لهذا التمييز الذي سوف يبنى عليه ثقافة محددة، إذ بدون إحداث اتصال بين الحاسوب وبين الإنترنت عن طريق وسيط ـ حتى الآن ـ لا يمكن القول بوجودنا على الإنترنت. وعليه فإن مجرد القول بارتكاب جريمة حاسوب لا يعني ضرورة وجودنا على الإنترنت، وإنما يكفي أن يكون الحاسوب في حالة عمل، في حين أنه لا يمكن القول بارتكاب جريمة من جرائم الإنترنت دون أن نكون على الإنترنت Online [1].

ومثل هذا القول نجده في القانون الأمريكي، حيث يميز القسم 18USC Sec. 1030، بين مصطلحي حاسوب Computer وبين حاسوب مشمول بالحماية Protected computer، فهذا الأخير يعني ذلك الحاسوب المتصل بغيره عن

(1) أن مصطلح Online يثير جدلاً، حيث أنه بالإنجليزية يشير إلى وجودنا على الإنترنت حيث إن ما يؤخذ في الاعتبار أن النظرة إلى الإنترنت كونها خط مفتوح يلزم لكي نصل إليها أن نكون على هذا الخط، في حين أنه إذا كان خارجها فإن المصطلح المستخدم هو Off Line.

طريق الشبكات / الإنترنت، في حين إن إيراد مصطلح حاسوب Computer فقط فإنه يعني مجرد الحاسوب غير المتصل بأي شبكة ولو داخلية (حيث يُعد هنا أداة تخزين فقط).

هذه الخصوصية التي منحها الحاسوب للإنترنت جعلتها تتميز في الحقيقة عنه من حيث الجزئية التي تعمل من خلالها، وإذا كان مثار اهتمام رجال القانون في زمننا المعاصر هو التعامل مع تفريع جديد في قانون المعلوماتية Droit Informatique، هو قانون الإنترنت Cyber Law، فهذا لا يعني في الحقيقة التعامل مع قانون الحاسوب Computer Law الذي يمثل أحد تفريعات قانون المعلوماتية أيضاً.

لذلك، فإننا نتجّه اتجاهاً آخر في هذا الشأن حيث نجد أنه من الصواب إحداث فصلٍ في هذا الإطار من حيث تعريفنا لجرائم الإنترنت تعريفاً منفصلاً عن جرائم الحاسوب، باعتبارها جرائم ناجمة عن استخدام الإنترنت، وهو التعريف المبني على فهم عميق لطبيعة المشكلة، من حيث ضرورة الفصل بين نوعي هذه الجرائم. حيث إن الإنترنت أفاءت على القانون بأشكال إجرامية جديدة لم تكن معروفة، حتى في ظل التجريم عبر الحاسوب، حيث إنه كنتيجة لظهور الإنترنت أضحت المشكلة ليست فقط إحداثيات التمييز في إطار التجريم عبر الحاسوب، في محاولة تتعدى منطق التبسيط إلى التعقيد (مثال جرائم الحاسوب ـ الجرائم المرتبطة بالحاسوب وتفصيلاتها أيضاً. . .إلخ). ولعل ما أنتهي إليه التطور الذي نراه سلبياً في توصيات مؤتمر G8 (الثمانية الكبار) عام 1998 ليدعو إلى مزيد من التأمل في هذا الشأن، إذ تمّ التوصّل إلى مصطلح High- Tech Crime أو جرائم التقنية العالية أو المتقدمة كنوع من محاولة التوسع في جرائم الحاسوب لكي تشمل الجرائم التي يكون الحاسوب طرفاً فيها كافة. وهذا كلّه يجعلنا نقرر أن هناك مفارقة مصطنعة بين جرائم الحاسوب وجرائم الإنترنت، على الرغم من الالتصاق الذي يكاد يكون طبيعياً بينهما.

وهذا الاتجاه الذي نأخذ به يجد له أساساً فقهياً يسعي إلى إقامة بنيان على النحو الذي يحقق مصلحة الإنسان قبل الآلة، إذ يذهب هذا الاتجاه إلى أن جرائم الإنترنت هي «كل فعل أو امتناع عَمْديّ ينشأ عن الاستخدام غير المشروع لتقنية المعلومات ويهدف إلى الاعتداء على الأموال المادية والمعنوية.

وعلى الرغم من التوجه الصحيح في تعريف جرائم الإنترنت على النحو السالف، سيما أنه يوضّح لزوم العَمْد، فقد كان هذا الرأي سباقاً على اتجاهات الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي المؤرخة 23/ 11/ 2001، فإن هذا التعريف لا يخلو من نقد، حيث يستلزم الامتناعَ كنشاطٍ مادي في مثل هذه الجرائم، وهو الأمر الذي لا يمكن تصوّره في هذا الشأن.

وعندنا يمكن وضع تعريف جامعٍ مانعٍ لجرائم الإنترنت، إذا أخذنا في الاعتبار ثلاث نقاط رئيسية، وعلى ضوئها يمكن وضع تعريف متكامل يفيد في تحديد الجرائم الناشئة عن الإنترنت.

**النقطة الأولى** : موضوع العالم الافتراضي Cyberspace (وبالفرنسية Cyberespace) الذي هو عبارة عن العالم المرئي The virtual world أو المجال الحيوي للبيانات وحركتها المعلوماتية، وهو العالم المختفي في الآلة التقنية[1]. والذي يطلق عليه الفقه العربي تسمية الفضاء الإلكتروني[2]، وهو العالَم الذي ابتكر فكرته كاتب الخيال العلمي الشهير William Gibson في روايته الشهيرة The Neu Romancer، التي أصدرها عام 1984، حيث وصف في هذا الكتاب فانتازيا إلكترونية Fantasy Electronic [3] تقابل فيها مجموعة هَكَرةٍ [= قراصنة]

---

(1) RCMP, op-cit.

(2) د. جميل عبد الباقي الصغير، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة 1999، ص 5.

(3) (NICHOLSON) Keith - International Computer Crime: A Global Village Under Siege - New England International & Comparative Law Annual 1996 - New England School of Law P. I. available online is Sep. 2001 at: http://www.nest.edu/annual/vol2/computer.htm.

من مَهَرَةِ الحاسوب، وطالَ نشاطُهم الاختراقَ والعديد من المظاهر التي تكاد تصل في بعض الأحيان إلى منطق الجريمة عبر الإنترنت، كما هي مقررة في التشريعات المعاصرة.

وإذا كانت الإنترنت لم يتم تعريفها بعدُ في النظم القانونية المقارنة بشكل مستقل، فإنه مع ذلك قد لجأت تلك النظم ـ بإيعاز من الفقه ـ إلى حيلة قانونية يمكن معها الحصول على تعريف قانوني لها، وذلك باستخدام مصطلح منبثق عن عالمها الافتراضي Cyberspace، وهذا المصطلح هو CyberLaw أي النظام القانوني للعالم الافتراضي للإنترنت، أو قانون الإنترنت، وهو «مجموعة القواعد القانونية التي تنظم العالم الفعلي للإنترنت»، وهي قواعد لم تزل بعدُ في طور النمو نتيجة لعدم إمكانية حدوث ملاءمةٍ بين المنظومة التقليدية للقانون وبينها، حتى وإن وصِفت بالغموض والإبهام.

وإذا كان قانون العالم الافتراضي/الإنترنت (Cyber Law)، لا يشكل عقبة في إطار بناء نظريته ـ إن أمكن تكاثف الجهود نظرياً على الأقل ـ فإن الحال غير ذلك فيما يتعلق بتطبيق هذه النظرية وتنفيذها، لا سيّما في النطاق القضائي، ذلك أنّ تركيبة قانون العالم الافتراضي/ الإنترنت ذات طبيعة مختلفة في الحقيقة عن تركيبة أي قانون آخر، فهو يتركب من طبيعة افتراضية ذات بُعدٍ دولي(1) يتطابق شكلياً مع مفاهيم العولمة، وليس مع المفاهيم التي يُعرّفها القانون الدولي، في الوقت الذي يتسع مدلوله ليشمل فروع القانون الأخرى. ذلك إنه من خلال مصطلح CyberLaw هرع الفقه المقارن ليضع تفريعات جدية لهذا المصطلح تعمل في إطاره ووفق فروع القانون المعمول بها، مثل

---

(1) TRANSNATIONAL NATURE OF CYBERSPACE, (CYBERCRIME AND CYBERPUNISHMENT ARCHAIC LAW THERATEN GLOBAL INFORMATION p. 2 report prepared by: McConnell INTERNATIONAL http://www.mcconnellinternational.com with support from WITSA http://www.witsa.com December 2000 availale online in dec. 2000, at: http://www.mcconnellinternational.com/services/cybercrime.html

Cyberbehavior للدلالة على سلوكيات القانون المدني، ومصطلح CyberCrime للدلالة على سلوكيات القانون الجنائي، ومصطلح Cybercommerce للدلالة على سلوكيات القانون التجاري، ومصطلح Cyberinvestigation للدلالة على الإجراءات الجنائية في إطار قانون الإنترنت، ومصطلح Cybertribunal على المحاكمات عبر الإنترنت. . . إلخ.

هذا الاتجاه الفقهي يسعى إلى إقامة علاقة بين القانون وبين الإنترنت، بمعنى إحداث ملاءمة بين الاثنين، بما يمكن معه تطويع القانون للإنترنت لمصلحة الإنسان في تعامله مع الآلة.

إن عملية إحداث ملاءمة بين النظام القانوني القائم وبين الإنترنت كانت قد برزت بدايةً حال موافقة الفقه النسبية على إمكانية التعامل القانوني مع الإنترنت بأسلوب التنظيم الذاتي للإنترنت Self - regulation، بحيث يجب ألا يكون هذا التنظيم هو الأداة الوحيدة وإنما يقبل، إلى جوار التنظيم القانوني بالأداة التشريعية، وجود أدوات تنظيمية نابعة من طبيعة الإنترنت، أي التقنية المعلوماتية. وإنّ سببية رفض وحدة التنظيم الذاتي كنظام قانوني للإنترنت يكمن في أن التنظيم الذاتي ليس مقنعاً بالدرجة اليقينيّة[1] بما يجعل العالم الافتراضي آمناً بالدرجة الكافية التي تسمح بالأمن والاستقرار[2]. على إن الأمر ليس على ذلك القدر من السهولة إذا تأملنا الاتجاه المضاد الذي يأخذ بضرورة التدخل القانوني لتنظيم العالم الافتراضي، حيث توجد لديه صعوبات أيضاً، من حيث إن أهم صعوبة تتمثل في تحديد طبيعة النظام القانوني الذي يحكم الإنترنت، وما إذا كانت النظم الأساسية في الدولة تكفي لحسم هذه الصعوبات وتذليل محتواها، أم إنّ العالم الافتراضي قام هكذا فجأة، وتالياً، يمكن أن يوجد له أساس في النظم

(1) RCMP, op-cit.

(2) CyberCrime And Cyberpunishment, archaic law threatens global information op-cit p. 2

القانونية المعاصرة، إلا أن العقل القانوني لم يستظهر هذا الأساس بعد. وهنا فإن المسألة تحتاج إلى مزيد من الوقت والتأمل والحكمة القانونية.

**وأما النقطة الثانية**: فهي ترتبط بالنتائج المترتبة في النظام القانوني حين فصل جرائم الحاسوب Computer Crimes عن جرائم الإنترنت CyberCrime، ومدى إمكانية قيام هذا الفصل تقنياً. والحقيقة إنه من الصعوبة بمكان فصل جرائم الحاسوب عن جرائم الإنترنت، نتيجة لارتباط الإنترنت بالحاسوب ارتباطاً تقنياً، إلا أن هذه الصعوبة سوف تتقلص كثيراً إذا أدركنا أن تقنية الحاسوب أعمّ بكثير من تقنية الإنترنت. فهو ـ أي الحاسوب ـ ثورة حقيقية ذات أبعاد اجتماعية وسياسية واقتصادية وقانونية ليس لها نهاية؛ إذ كما أنتجت تقنية الحاسوب الإنترنت، فإن ذلك لا يعني نهاية المطاف في هذا الشأن، حيث المؤشرات السائدة تشير إلى أن تقنيات جديدة للحاسب يتوقع أن تظهر في الأفق قريباً، وتدليلاً على ذلك فإن دولاً مثل كندا تربط جرائم الإنترنت بجرائم الاتصال عن بعد Telecommunication Crime التي يمكن أن يحدث بوساطة الإنترنت مثلما يمكن أن تحدث بوساطة الهاتف وجهاز الموجات الصغيرة Microwave والأقمار الصناعية Satellite وغير ذلك[1].

وإذا كان حقيقياً أن تقنية الحاسوب قد انطلقت لكي تبتكر الإنترنت، فإن منطقة الخلاف بين العمل السلبي الذي يكون محله الحاسوب، وبين ذلك الناجم عن استخدام الإنترنت، يُعدّ أحد الصعوبات الجديدة التي تواجه فقه القانون حقيقةً، فإذا تحدد هذا التعريف فإنه من السهولة التوصل إلى بحث التوجه السياسي والتشريعي في دولة ما. لأجل ذلك نجد إن البعض لا يمانع في إطلاق صفة جرائم الحاسوب Computer Crime على الاختراق Hacking إلا

---

(1) FGSSC - available online in feb 2000 at: Http://www.usdoj.gov/criminal/cyber-crime/search docs/toc.htm.

أنه يشترط بالضرورة أن يكون الحاسوب مرتبطا بشبكة Connected [1] أو Protected Computer، ويمكن القول إجمالاً، إن هناك اتجاهين في إطار رصد تعريف جرائم الإنترنت؛ الاتجاه الأول ينحو منحى التعريف المضيق الذي يقوم برصد جرائم الإنترنت في ربط جرائم العالم الافتراضي ككلّ بالحاسوب، حيث يذهب هذا الاتجاه إلى «إن مصطلح العالم الافتراضي مرجعه استخدام الحاسوب لتسهيل ارتكاب الجرائم[2]، وهو تعريفُ مضيق لكونه يربط إجرام العالم الافتراضي بالحاسوب بالمفهوم الضيق، حيث أن مصطلح الحاسوب يتسع إلى أبعد من ذلك الذي نعرفه اليوم، وبحيث يجب الأخذ في الاعتبار تلك النظرة المستقبلية للحاسوب التي تعني حَوْسَبَةَ أو رقميّةَ العالم البشريّ على النحو الذي يحقق اعتماد الإنسان عليه في كل شيء. لذلك، فإن النقد الذي يمكن توجيهه إلى هذا التعريف، أنه يربط تعريف جرائم الإنترنت بالحاسوب، فإن ذلك يعنى أنّ فصل الحاسوب عن الإنترنت في أبسط مظاهر هذا الفصل (أي بفصله بعدم الدخول إلى الإنترنت ـ أو بفصل الكهرباء عنه) يعنى انتهاء الجريمة وعدم اتصالها بنا، في حين أن ذلك غير صحيح، إذ تظل الجريمة قائمة وظاهرة في أماكن أخرى.

لذلك، فإن الأرجح هو الاتجاه إلى التوسّع في تعريف جرائم العالم الافتراضي/الإنترنت، ومكمن التعريف الموسّع هو السعي إلى بحث استقلاليةٍ لجرائم الإنترنت تتنافى مع ربطها بالحاسوب وجرائمه. ولما كنا فيما سبق، قد عرّفنا الإنترنت أنها في الحقيقة الجرائم الناشئة عن استعمال هذا التواصل بين

---

(1) Nicholson - International computer crime op - cit P.2

(2) (KATYAL) Neal Kumar - criminal law in criminal law in Cyberspace, Georgetown University law center 2000 P.13 A revised version of This working paper is forthcoming in the university of Pennsylvania law review Volume 149 April 2001 This paper can be downloaded without charge from the social science research Network Electronic paper collection at Http://papers.ssrn.com/ aperitif abstract id = 249030 working paper No 249030.

الشبكات، وهذا اتجاه المُشرِّع الأوروبي في اتفاقية الجريمة عبر العالم الافتراضي المؤرخة 23/ 11/ 2001، وكذلك اتجاه المُشرِّع الأمريكي حين رَصْدِه لمصطلح Protected Computer، ولما كان التقسيم الأمثل لهذه الشبكة إلى ثلاثة أقسام، كما عرضنا لذلك فيما سلف (شبكة المعلومات الدولية ـ البريد الإلكترونى ـ الاتصال المباشر)، فإن العدوان باستخدام الإنترنت من خلال أقسامها هو الوضع الصحيح الذي يجب أن يكون عليه التجريم هنا. لذلك نجد إن جرائم الإنترنت في حقيقتها هي تلك الجرائم التي ترتكب بدوامِ التواصل بين الشبكات.

وإذا كان هذا التعريف يتميز بالعمومية إلا أنه مع ذلك يظل محصوراً في إطار الإنترنت، لذا فإنّ كل جريمة من الجرائم كانت وسيلتها الإنترنت أو أقسامها إنما هي من جرائم الإنترنت.

إن التعريف الذي نقول به يجعلنا في الحقيقة نعترف مُسبقاً بأن ظاهرة الإنترنت لا تزال غامضة في دراسات القانون. وفى هذا الإطار رصد المرشد الفيدرالي الأمريكي لتفتيش وضبط الحاسوب Federal guidelines for searching and computers أهمية الاعتراف بأن رجال القانون بدأوا في مواجهة مشاكل جديدة على أثر إنجاز ثورة معلومات الحاسوب والاتصالات في القرن الواحد والعشرين[1].

إن الفصل بين الحاسوب وبين برمجياته يُعدّ تدليلاً على قيمة الفصل بين الحاسوب وبين الإنترنت. ولقد اشتدّ الصراع ـ بناءً على ما سلف ـ بين فقه القانون وخبراء تكنولوجيا المعلومات حول الأبعاد الفلسفية لتحديد جرائم الإنترنت أو جرائم العالم الافتراضي، ما بين مؤيد لاعتبار هذه الجرائم مجرّد جرائم عادية ترتكب بوساطة الحاسوب وآلياته ـ وهو الأمر الذي يترتب عليه تطبيق القانون السائد عليها، وبما لا يخرج عما هو مقرر في هذا الشأن، كما أنه

(1) Theoumyre - abuse in the cyberspace, op-citP.8.

يقود إلى القول بكفاية النصوص الجنائية للانطباق عليها لكونها لا تتعدى ما هو مقرر حين اختراق القانون الجنائي، كما هو الشأن في الانتهاك Trespass والاختلاس larceny والقرصنة Conspiracy ـ وبين مؤيد لاعتبار جرائم الإنترنت إنما هي جرائم ذات أبعاد جديدة وتحتاج إلى إعادة نظر في هيكلة القانون الجنائي الحالية، ويدلل هذا الاتجاه على ذلك بموضوعات القانون الجنائي وصعوبة الإثبات، وكذلك حالة مرتكبي جرائم، أو ما يطلق عليه مشكلة الهَكَرَة Hacklers في هذا الإطار(1). وإذا كان هذا الاتجاه له منطقه في ضرورة التعامل مع جرائم الإنترنت بخصوصية ما، إلا أن عملية الكشف عن هذه الخصوصية التي تتمتع بها هذه النوعية من الجرائم استلزمت ضرورة التطرق إلى الخصوصية التي تمتع بها الإنترنت ذاتها. وأما النقطة الثالثة؛ التي يجب الانطلاق منها للتأكيد على تعريف جرائم الإنترنت من منطلق أنها جرائم ترتكب بوساطة تلك الوسيلة أو الأداة التواصلية بين الشبكات دونما اعتبار للحدود الدولية، تتعلق بكينونة الإنترنت كظاهرة لها ايجابياتها وسلبياتها، فإنه يجب معاملتها على هذا الأساس، مثلها في ذلك مثل الظواهر الجديدة. لذا فهي ليست مجرد وسيلة لارتكاب الجرائم، وذلك لما توفره من مجموعة بدائل مختلفة عبرها، حيث انه يمكن ارتكاب الجرائم بوساطة البريد الإلكتروني مثلاً (الذي يحتوى على مجموعة بدائل مختلفة) كما يمكن ارتكاب جرائم عبر البدائل التي توفرها شبكة المعلومات الدولية. . . الخ

ومن هذا المنطلق، إن الرؤية المحددة للإنترنت لا تنطلق من الفكر النظري وإنما من الواقع العملي، وهذا يستدعى البحث في مدى استعداد المجتمع للتقبل الفكري لها، إذ هي مجال حيويّ Atmosphere في المجتمع

---

(1) Eric J. Sinrod and William P.reilly- Crimes: A practical approach to the application of federal computer crime laws P.3 Santa Clara computer and high technology law Journal may 2000 Volume 16, Number 2.

قابل لربط عقليته Mentality بها؛ ففي بعض الدول التي مرت بتجارب واقعة على الإنترنت أمكن لها أن تُحدِث تفاعلاً إيجابياً يتواصل مع قانون الإنترنت مثلما حدث في الفيليبين على أثر قيام أحد طلبة الجامعة هناك بابتكار فيروس الحب I love You فقامت الدولة بتكثيف جهودها لسن قانون في هذا الشأن، سيّما بعد التدخل الدولي نتيجة لكون الضرر عبَرَ الحدود الدولية إلى نطاق عالمي، فأصاب أجهزة حاسوبٍ حول العالم.[1] فالعالم الفعلي هو جزء من عالمنا غير منفصل عنه، لذلك فهو ليس بعيداً عن إمكانية إحداث تنظيم قانوني له[2]، بل إن الفقه ينادي بكينونة عقلية منفردة للإنترنت، فَعَلا مبدؤه عالميةَ التفكير وإقليمية الحركة[3].

## تحرر الإنترنت من قيود التقنية

يمكن القول إجمالاً، إنه إلى حين اكتشاف شبكة المعلومات الدولية www على يد مهندس الاتصالات الأنجليزى Lee عام 1991، لم تكن الإنترنت شائعة الاستعمال بل كانت محاطة بنوع من الخصوصية تتعقب باستخداماتها الحصرية على الممارسين للحاسوب، وكان مرتادوها يخضعون لنظام أمنيّ ما، إلا أنه بعد ذاك العام (1991)ـ وسياسياً بعد سقوط الاتحاد السوفييتي انطلقت الإنترنت إلى السطح لتجد أصنارتها يتزايدون يوماً بعد يوم.

ولقد أدى هذا الانطلاق إلى علنية الانترنت، فلم تعد السرية ذات شأن، وترتّب على هذا التحرر من السرية أمران، الأول سهولة استخدامها، والأمر الثاني هو سهولة تطورها.

---

(1) Cyber crime And cyberpubishment, archaic law threatens global information op - Cit P.4.

(2) Rcmp op-cit «a computers and telecommunications explode into the next century prosecutors and agents have begun to confront new Kind's explode into the next century prosecutors and agents have begun to confront new Kind's of problems».

(3) Thoumyre - abuse in the cyberspace op-cit P.9 : Think Globally and Act locally.

فمن ناحية نجد الإنترنت أداةً سهلة الاستخدام، أو الاستعمال، طالما كان هناك حدّ أدنى من القدرة على استخدام تقنية الحاسوب. وتجدر الملاحظة هنا أن المقصود ليس هو الحاسوب فقط، وإنما تقنية الحاسوب ككل، ما يعنى أن هذه التقنية قد وصلت إلى أبعد من كونها محلّ استخدامٍ عَبْر الحاسوب فقط، وإنما من الممكن أن تكون عبر أجهزة الهاتف النقال والمِرْئاء T.V وغير ذلك.

ومثل هذه الأدوات أصبحت سهلة الاستخدام من قبل الجميع، فهي تقنية ليست بعيدة المنال عن المعرفة الإنسانية العامة، ويكفى أن نورد المثال التالي : ففي إطار الحاسوب الشخصي Pc فإنه بعد أن كانت عملية تشغيله تحتاج إلى قدرات تقنية خاصة، توصلت صناعته الآن إلى إمكانية القيام بعد أن قامت بتشغيله دونما صعوبة تذكر، بل وباستخدام الأوامر الصوتية أيضاً من دون الحاجة إلى تشغيل الجهاز بالمعرفة التقنية.

ولقد لازمَ التطورَ في تقنية الحاسوب تطورٌ ايداعيٌّ في سهولة استخدام الإنترنت، إذ يمكن لأي شخص أن يُعدّ جهازه لكي يستدعي الإنترنت بمجرد تشغيله وأن يُجرى عملية بحث بسهولة تامة عبر الإنترنت؛ وفى هذا يميز القانون بين الحاسوب المتصل بالإنترنت؛ ويطلق عليه في المصطلح Protected Computer، وبين الحاسوب غير المتصل بالإنترنت، وفي هذه الحالة فإن المصطلح المستخدم هو Computer فقط، كما أشرنا إلى ذلك آنفاً. وإذا تأملنا القدرة الاستيعابية لاستخدام الإنترنت لوجدنا أن غالبية مستخدمي الإنترنت ليس لهم دراية كبيرة باستخدامات الحاسوب وإنما بتشغيله في إطار ضيق فقط، إلا أنه عبر الإنترنت فإن الملاحظ أنهم يملكون القدرة على التصفح والمراسلة والمجادلة أو الاتصال المباشر عبر الإنترنت، ولقد ترتب على ذلك أن وجدت تقسيمةٌ بين مستخدمي الإنترنت إذ يُمَيَّز بينهم من حيث التعامل بالإنترنت وبين الحصول على خدماتها

فالتعامل بالإنترنت يحتاج إلى قَدْرٍ من الدراية بتقنيتها، فضلاً عن تقنية

الحاسوب ذاتها، وهو مجال للتخصص العلمي في مستوياته كافةً. على إنه من الممكن أن يكون هذا التخصص مجاله التعليم دونما حاجة إلى دراسات في مؤسسات متخصصة في حين أن خدمات الإنترنت services تشكل الغالبية العظمى من مستخدمي الإنترنت، بما في ذلك سلوكيات الإنترنت. ويلاحظ هنا أن استحداث تمييز بين التعامل بالإنترنت وبين خدماتها، له قدر كبير من الأهمية في مجال التجريم والعقاب؛ إذ يمكن من خلاله استحداث تمييز جنائي بين تجريم التعامل غير المشروع بالإنترنت من قبل المتخصصين، وبين تجريم الباحث عن خدماتها الذي يكون في العادة غير متخصص فيها وإنما هو مجرد شخص عادي ـ توجد لديه خاصية استخدام أو استعمال الإنترنت ـ يرتكب جرماً عبر الإنترنت. يمكن القول هنا إن للصدفة دورها المؤثر في الغالب الأعمّ، والمثال العملي الدارج هو عملية الولوج مصادفة من قبل أحد المستخدمين إلى صفحة مُشفّرة أو إلى حساب بريد الكتروني دون أن يكون قاصداً ذلك، فمثل هذا النشاط المادي لا يمكن الجزم بكونه عمداً أو خطأً، وكذلك لا يمكن تصورّه في نطاق الجريمة المحتملة التي تستلزم قَصْدَ ارتكاب جريمة أصلية، وإنما يمكن أن يثار من جديد موضوع المُجرَّم بالصدفة، وهو مثار نظرية لومبروزو الوضعية.

ومن ناحية أخرى فإن أثراً هاماً ترتّب على تحرر الإنترنت من قيود السرية، ويتعلق هذا الأثر بمسألة تطوير الإنترنت. فقد انفتح المجال في تطوير الإنترنت لكائنٍ من كان، فلم يعد المجال محصوراً في طائفة العلماء، ولقد ساعد على ذلك اللامركزية التي تتمتع بها الإنترنت، فكل من يملك الأفكار المبدعة يمكنه تنفيذها عبر الإنترنت، لذلك نجد الإنترنت محلاً لصراع قوي بين الأفكار المبتكرة والمبدعة والمتطورة لدى طوائف ليست من فئة العلماء، بل بمكن التأكيد هنا على أن الإنترنت مَرْتعٌ خصبٌ للأفكار العلمية الجديدة، سواءٌ كان ذلك في مجال التعامل بالإنترنت أو في مجال خدمات الإنترنت.

والاعتقاد بسهولة تطور الإنترنت أمر له خطورته، إذ سوف تستفيد البشرية من تطوير الإنترنت بما يؤدي ـ دائماً ـ إلى سهولة استخدامها، وبما يوفره هذا التطوير المستمر من إمكانات ضخمة للتعامل مع الإنترنت. إلا أنه مع ذلك قد يكون سلوك التطوير المستمر هذا عرضة لمساءلة القانون إذا علمنا إن التطوير قد يكون مبعثه التعجيل به. ومعلوم أن الجانب السلبي يوفر الكثير من الوقت والجهد في تطوير الأمور فاختراق أنظمة أو شبكات يحتاج إلى مهارات متخصصة للمخترق، وهو يحتاج إلى دراية بالحاسب والبرمجة ثم إلى دراية مكثفة بالإنترنت وطرائق التكنولوجيا والتعامل معها، ثم بعد ذلك يحتاج إلى اختراق التشفير والحصار الأمني المشيّد حول الشبكات للولوج إلى داخلها. كل هذه أمور تحتاج إلى إعداد وتدبير مسبق، وتفكير مدبّر، وإدراك للتقنية عبر الحاسوب والإنترنت، ثم كيفية التعامل مع طرائق التشفير. وهذا كله، وإن كان يمثل الجانب السلبي المحظور، وقد يصل إلى التجريم، إلا أنه مع ذلك ينمّ عن استخدام عقلي للتقنية الحديثة، قد يفيد بشكل أو بآخر في تطوير الإنترنت، وهذا أمر أدركته الشركات والهيئات الكبرى، حتى إنها تسعى إلى التعاقد مع هؤلاء لأجل تحقيق مصلحتها في الاستفادة منهم كتقنيين، ثم تفادي ارتكابهم جرائم وأفعال غير مشروعة عبر الإنترنت.

### الفرع الثالث: التأثير الاجتماعي الاقتصادي للإنترنت

الإنترنت ـ كما أسلفنا ـ تعدّ فعلاً غربية تجاه التطور العلمي الشرقي، وردّة الفعل هذه كانت من القوة بحيث ـ وفيما يبدو ـ قصمت ليس فقط ذلك التطور العسكري الشرقي، وإنما أيضاً كل تأثير للسِرّية في علوم المخابرات. فلم تعد المشكلة ـ بعد ظهور الإنترنت ـ خشية افتضاح السرّ، بل كيفية التوصل إلى القدرة على كتمانه واستمراريته في وعاء السرية ؟

ولقد كان لبزوغ شمس الإنترنت تأثير اجتماعي اقتصادي ذو طابع عالمي، إذ أحدثت هذه التقنية الجديدة تحوّلات في الأفكار السائدة، بل إنها جعلت هذه

المرحلة من التحولات تطال المستويات كافة وذلك لتأثير الإنترنت على المجتمع والاقتصاد، حيث امتدت تلك التحولات لتصل إلى صُنّاع القرار السياسي في كل دولة، وكان لهذا الامتداد شأن عالمي أيضاً.

ولما كانت الحالة الاجتماعية الاقتصاديةُ تعدُّ المعدّلات التي يُقاس على ضوئها التطور والتخلّف في العالم المعاصر، فإن التعرض لها يجعل هذه الظاهرة تبرز أكثر وضوحاً وفهماً. فمن الناحية الاجتماعية برز تأثير الإنترنت كظاهرة عالمية على المتجمع الدولي والإقليمي بل والمحلي أيضاً؛ فالحياة غَدَتْ أكثر سهولة عبر الإنترنت، وإذا كان الحاسوب وما أحتلّه من هيمنة في الجانب الاقتصادي لم يؤدِّ المُناطَ به في الجانب الاجتماعي كاملاً، فإنه يمكن القول إن الإنترنت قامت حقيقة بهذا الدور لتمنح الحاسوب دوراً اجتماعياً وهي لمّا تزَلْ بعدُ في مهدها.

لقد فرضت الإنترنت ذاتها على الرغم من إنها مجرد ردّة فعل غريبة تجاه تقينه عامة سبقتها. ولكن كيف يتأتّى لردّةِ فعلٍ أن تفرض نفسها بعموميةٍ على النحو الذي هي عليه الآن.

من الصعوبة بمكان التبرير بأن هناك توجهاً سياسياً إيجابياً تجاه الإنترنت، إذ إن مثل هذا الأمر لا يستمرّ، فهو وإن حدث فعلاً فإنه لا يستمر في العادة سوى فترة قصيرة بتأييد قوة القرار السياسي ثم تهفت خطاه حال تغاير موضوع القرار السياسي واعتراكه في النواحي الاجتماعية الاقتصادية. كذلك من الصعوبة بمكان اعتباره نصراً علمياً، لأن النصر العلمي الحقيقي، والذي اعترفت به الإنسانية، هو الأساس الذي بنيت عليه فكرة التقنية الحديثة. كان اكتشاف الكهرباء على يد توماس إديسون. ولكن من السهولة بمكان التعرف على الكيفية التي فرضت بها الإنترنت ذاتها إذا تأملنا الجانب الإحصائي من زاوية التعامل الإنساني مع الإنترنت؛ والقاعدة هنا أنه طالما كان هناك لجوءٌ إلى الافتراض في

المجال الإحصائي، فإن معنى ذلك هو عدم تراجع وكذلك عدم استقرار الجانب الإحصائي ذاته، إذ إنه في زيادة أو تزايد مستمر، فإذا وصلنا إلى رقم معين الآن فإنه بعد ساعة لا يمكن الجزم بمقدار الزيادة الممكنة هنا؛ وهذا الأمر هو ما يحدث عبر الإنترنت، حتى أن السيدة J. Reno النائب العام الأسبق للولايات المتحدة الأمريكية لم تجزم بعدُ برقم محدد وإنما تقريبي أو افتراضي في مقالاتها كافة على التأثير الاجتماعي للإنترنت في هذا الشأن. وهناك حيلة عملية يمكن اللجوء إليها للتعرف على التأثير الاجتماعي للإنترنت؛ إذا قمنا بها فإننا سوف نجد أنه لا تخلو دقيقة واحدة من الحركة عبر الإنترنت، حتى في فرضية عدم وجود أخذ الآن على الإنترنت، فكيف عرفنا بذلك؟ لأننا الآن على الإنترنت Online وهذا يعنى أن أحداً ما هناك. فالإنترنت مجال استقطابي نشط ووسيلة علمية ممتعة لفتح مجالات جديدة، فالذي يملك وقت فراغ من أي نوع ويكاد يصاب بالملل، يستطيع الولوج إلى الشبكة فتنفتح له آفاق عن أفكار جيدة وعلاقات إنسانية متكاملة. وحيلة أخرى يمكن اللجوء إليها من قبل طلاب العلم ومُعدّي البحوث، إذ أصبح في مقدور الباحث الحصول على المعلومات المطلوبة بمجرد إجراء عملية بحث Search حيث يتم رصد مضافة إلى البحوث والموضوعات المتعلقة ببحثه طالما وجد لها مكانا على الإنترنت، إذ تتهافت المؤسسات ذات الطابع العلمي على وضع صفحات تتضمن بحوثات ودراسات علمية.

ومن أهم مظاهر التأثير الاجتماعي للإنترنت من ناحية (شبه اللغة) التي يتم التعامل بها عبرها ـ وهو أمر جعلنا نتوقف كثيراً عنده؛ فإذا كانت إحدى لغات التعامل بالإنترنت Html-Java هي في حقيقتها ليست لغة من الناحية العلمية وذلك كنتيجة لصغر مكوناتها، حيث جعلها هذا الأمر مجرد رموز تحتاج إلى صيغة تحويلية حتى تتخذ موضعها على الإنترنت، فإن مثل هذا الأمر فرض حقيقة موضوعية لا مجال لأن يتطرق إليها شك، وهي عدم إمكانية الجزم أو

المفاضلة بين اللغات الإنسانية عبر الشبكات، إذ بمقارنة حجم المعلومات المرصودة عبر الإنترنت واللغة المستخدمة فيها يكون التقدير وهذا أمر لا يمكن الجزم باستقراره. فإذا كانت اللغة الانجليزية الأكثر شيوعاً واستخداماً عبر الإنترنت، فإن ذلك لا يعد مقياساً على ان السيادة للغة الانجليزية عبر الإنترنت، إذ من الممكن إحياء اللغة الهيروغليفية الفرعونية القديمة عن طريق نشر وثائق الفراعنة وذلك أكثر تعداداً مما وصل إليه نشر البحوث بالانجليزية عبر الإنترنت، فهل يعنى ذلك أن الإنترنت تصبح فرعونية؟

ومن الناحية الاقتصادية برزت الإنترنت بقوة في المجال الاقتصادي، ويمكن القول إجمالاً أنها نتخذ بدايتها ـ وهي لا تزال بعدُ في مهدها أصبحت مؤثرة في الاقتصاد العالمي. فحتى سنة 2000 كان حجم التجارة عبر الإنترنت ثلاثة تريليونات دولار أمريكي، وأصبح مصطلح التجارة الإلكترونية Electronic Commerce يتم تداوله بشكل مكثف سواءٌ على المستوى الأكاديمي أو العملي، فالتجارة الإلكترونية حقيقة واقعة الآن[1] على الرغم من مشكلاتها التقنية المتواصلة، وليس مفهوم التجارة الإلكترونية مجرد عرض السلع كما هو الشأن في أسلوب Tele-Achat [2]باستخدام الأجهزة التقليدية كالمذياع Radio والقناة T.V والذي له سوق رائجة في العالم العربي[3] بل يمتد عبر الإنترنت إلى إمكانية تداول السلع والخدمات كما هو الشأن في تداول البرمجيات والوثائق والمعارف

(1) (BABY) Eric - le droit du commerce electronic da la protection al confiance - revue de droit de l’information et des telecommunications 2 juin 1998 available in Feb 2000 at:

(2) وهو أسلوب عرض السلع والتسوق عير شاشات التلفزة وأيضاً الإذاعة المسموعة الذي بدأ أول مرة في فرنسا.

(3) د. أحمد السعيد الزقد ـ حق المشتري في إعادة النظر في عقود البيع بواسطة التليفزيون ـ مجلة الحقوق، السنة 19 عدد 3 مجلس النشر العلمي / جامعة الكويت سبتمبر 1995 ص 180.
أنظر كذلك:

(VERBIEST) Thibault - comment conceiver la distribution selective et internet? - Juriscom Feb. 2000 at http://www.juriscom.net/espace2/2/ce0218.html

التي يمكن نشرها بلغة الإنترنت، وباستخدام نُظُم التحميل Upload والإنزال download خلال مدة زمنية قصيرة.

ويمكن، في الإطار الاقتصادي أيضاً، الحصول على نظام خدمي متكامل إذ بالإمكان متابعة البورصة العالمية لمعرفة تطورات الأسعار وتبادل الأسهم، فالمتابعة وقتية وليس هناك مفارقة في الزمن، وسوف تسمح الإنترنت بالتكافؤ الاقتصادي فيما يتعلق بدراسة حالة السوق العالمية نتيجة للتقارب المكاني والزمان الحادث بسببها، فيمكن متابعة الحسابات المالية والقيام بالعمليات المصرفية واستخدام البطاقات الإلكترونية للسداد والحجز في الفنادق وشركات الطيران وتأجير وإيجار العقارات والمنقولات والبيع والشراء.. إلخ، كل ذلك في فترات زمنية قصيرة للغاية. وأكثر ما يدل على التأثير الاقتصادي للإنترنت أنها سمحت بظهور أفكار اقتصادية جديدة ـ هي بالتأكيد محل نقاش وجدل على جميع المستويات ـ ومنها ظهور المحل الإلكتروني E-store في أي شكل كان فهو محل تجارى ليس له أرضية مادية في الواقع، وإنما مجرد صفحات على الإنترنت ويجد رواجاً في التعامل عبره مثلما هو الحال في نشر المؤلفات والسمسرة التي تجد لها متنفساً هائلاً عبر الإنترنت، لا سيما وأن دور الوسيط التجاري هو دور معنوي في الأساس، ومثل هذا المحل الالكتروني سوف يكون عرضة لانفجار قانوني في المرحلة المقبلة، لا سيما وأن روح المنافسة عبر التجارة الإلكترونية تأخذ مكانها بقوة. إن التطور الذي سوف يصاحب الإنترنت كما هو الشـأن في مشروع ميثـاق الإنترنت Charte de Internet الصادر في فرنسا عام 1997 والذي يتضمن قواعد سلوك لمستخدمي إنترنت Regales 1997 et usages des abettors de internet eb France على أن أبرر مظاهر تأثير الإنترنت في الحياة الاقتصادية عالمياً ومحلياً يظهر في الربط بين الاقتصاد والفنون، فكلما تقدمت تقينه الحاسوب ازدادت معدلات النمو في التعامل بالإنترنت إذ إن إعداد صفحة قديماً، زيادة عن تكلفتها الكبيرة آنذاك ـ كان من

الصعوبة بمكان إلحاق رسومات وزخرفة فنية وألوان فيها بل وحتى إضافات متعددة، هذه الأطر أبرزت إمكانات وقدرات تقنية جديدة ذات طابع ابتكاري في صورة اقتصادية، وفتحت آفاقاً جديدة للعمالة وسوق العمل الدولي. ويبرز هذا القول كثيرا إذا تأملنا الجانب الدعائي Advertising ما تحققه سوقه الرائجة عبر الإنترنت، حتى أن التطورات الهائلة في أساليب الدعاية والإعلان عبر الإنترنت ربما كانت سبباً مباشراً في تطوير برمجيات الحاسوب المتعلقة بالرسومات والتصميم، ومن ثَمّ برزت النواحي الاقتصادية في الجانب الدعائي لتشكل سوقا عالية الجودة. إذ من الناحية النفعية تحقق التقنية نتائج إيجابية غير متوافرة في الإعلان عبر الإنترنت أعلى معدلات التأثير الاقتصادي والربحي بما تحققه التقنية من إيجابية غير متوافرة في الإعلان في عالمنا المادي، مثل تقنية Abbots التي تجعل برمجيتها تلتصق برغبات أعضاء الإنترنت وتتبعهم بأحداث ما يستجدّ وفق رغباتهم دون حاجة لمتابعتها حتى تأتي إلى الشخص أولاً بأول.

إن المبادئ الجديدة التي تضعها في الفكر الاقتصادي لا تحكمها أفكار اليمين واليسار، بل هي أقرب إلى طريق ثالث، وتنهض فكرة أن جميع أعضاء الإنترنت لهم حظ فيها، وليس من مفاضلة بين الجميع إلا لمن يملك القدرات والتقنيات ومن يتفاعل مع التطور العلمي الذي لا يمكن التراجع عنه. وعلى الرغم من التحولات الإيجابية التي استهدفتها الإنترنت اجتماعياً واقتصادياً، فإن هذه التحولات الإيجابية صادفت وجود نقيضها السلبي متوافراً، وربما هذه الوفرة قادرة على إحداث جدل واسع النطاق بدأ من نقطة الصفر فيما يبدو، أي أن الجدليةُ مثارة حول واقع الإنترنت على المستويين الاجتماعي والاقتصادي معاً. فقد برزت النواحي السلبية في هذين الاتجاهين بشكل خطير وشرعت المحاكم في النظم المقارنة بالتصدي لدعاوى متعلقة بأعمال الإنترنت بناءً على ما أرساه المشرِّع من تشريعات وما يتراءى لها من أعمال واقعية في محاولة شديدة الخطورة على النظم القانونية القائمة. فقد مسّت الجوانب السلبية

للإنترنت نواحي لم يكن في الحسبان وجودها يوماً ما، ولقد أدى هذا الأمر إلى قيام فقه القانون ورجال القضاء في النظم المقارنة بمحاولات جادة لدعم البدايات في هذا الشأن. ولقد كان السؤال يدور حول البحث في مدى إمكانية إحداث مواءمة بين النظام القانوني ومن ثَمَّ النظام الوضعي وبين الإنترنت، وربما نتائج هذه المواءمة ؟

إن مدى الأهمية التي تقوم عليها التجارة الإلكترونية (عبر الانترنت) دفعت الإدارة الأمريكية في عام 1997 إلى إعداد (نموذج عمل للتجارة الإلكترونية العالمية، ولقد أخذ هذا النموذج الرئاسي الأمريكي (كلينتون ـ أل. . .جور) طابعاً متطرفاً من حيث تضمنه خمسة أسس رئيسية لترشيد تنمية التجارة عبر الإنترنت. على أن أبرز مظاهر النموذج المذكور كونه لم يوضع كتوجيه للحكومات حول العالم وإنما احتوى على ما يجب على الحكومات عدم فعله[1].

ويشتمل ذلك على ثلاثة عناصر :

1 ـ يجب أن تكون القيادة للقطاع الخاص.

2 ـ على الحكومات أن تتجنب التقيد المفرط under restriction الذي يؤدي إلى تشويه تطور ساحة السوق الإلكترونية.

3 ـ على الحكومات أن تعمل على تشجيع البيئة القانونية القابلة للتنبؤ Predicable والتماسك consistent في الحدود الدنيا Minimalist.

---

(1) (Macintonch) Kerry Lynn. The New money the Berkeley technology law journal vol.14/ 2 P.1.
http:// law.berkeley.edu/journals/btlj/articles/14/2P.1
http://law.berkeley.edu/journals/btlj/articles/14/2/macintoch/text.html.
A Framework for Global electronic commerce 1997 available online in may 2000 at http://www.iitf.nist.gov/eleccomm/eccomm.html.

# الفصل الثاني

# الجرائم الرقمية والمعلوماتية

## مفهومها وأسبابها وأنواعها وخصائصها

لقد أفرزت ثورة الاتصالات والمعلومات وسائل جديدة للبشرية تجعل الحياة أفضل من ذي قبل؛ غير أنها فتحت الباب على مصراعيه لظهور صور من السلوك المنحرف اجتماعياً التي لم يكن من الممكن وقوعها في الماضي؛ وتخرج عن دائرة التجريم والعقاب القائمة ؛ لأن المشرِّع لم يكن من الممكن أن يتصور حدوثها أصلاً .

فمن جهة أولى أتاحت نظم الكمبيوتر (الحاسوب) ظهور صور جديدة من الجرائم لم تكن موجودة في الماضي ؛ وذلك مثل سرقة المعلومات والأسرار المودعة في قواعد المعلومات . ومن جهة ثانية أتاحت هذه النظم الفرصة لارتكاب الجرائم التقليدية بطرق غير تقليدية ؛ كما هو الشأن بالنسبة لجرائم الغش وإتلاف وإفساد المعلومات المخزنة في قواعد المعلومات .

ومن ثَمّ ينقسم هذا الفصل إلى ثلاثة مباحث، تناول المبحث الأول تعريف الجريمة المعلوماتية، واختصّ المبحث الثانى بالحديث عن أسباب الجريمة المعلوماتية وخصائصها والمجرم المعلوماتى، وجاء المبحث الثالث

مرّكزاً على تصنيـف جــرائم المعلوماتية والإنترنت، وأخيراً عكف المبحث الرابع على قضية انتشار الفيروسات المعلوماتية وأساليب الوقاية منها.

## المبحث الأول:
## تعريف الجرائم الرقمية والمعلوماتية

تعددت التعريفات التي تناولت الجريمة المعلوماتية، ويرجع ذلك إلى الخلاف الذى أثير بشأن تعريف هذه الجريمة ومن قبلها تعريف المعلومة ذاتها؛ فالجرائم المعلوماتية هي صنف جديد من الجرائم، ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين انتقلوا بالجريمة من صورتها التقليدية إلى أخرى إلكترونية قد يصعب التعامل معها، لأن الجريمة المعلوماتية هي من الظواهر الحديثة؛ وذلك لارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات. وقد أحاط بتعريف الجريمة المعلوماتية الكثير من الغموض حيث تعددت الجهود الرامية لوضع تعريف جامع مانع لها ولكن الفقة لم يجتمع على وضع تعريف محدَّد لها بل إن البعض ذهب إلى ترجيح عدم وضع هذا التعريف بحجة أن هذا النوع من الإجرام ما هو إلى جريمة تقليدية ترتكب بأسلوب إلكتروني.

وعلى أية حال، فإنه على الرغم من تنامي جهود التصدي لظاهرة الإجرام المعلوماتى، إلا أنه لا يوجد تعريف محدد ومتفق عليه بين الفقهاء حول مفهوم الجريمة المعلوماتية، فقد ذهب جانب من الفقه إلى تناولها بالتعريف على نحو ضيق وجانب آخر عرّفها على نحو موسّع.

### التعريف الضيق للجريمة المعلوماتية

ذهب الفقيه (merwe) إلى أن الجريمة المعلوماتية هي الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي ـ أو هو الفعل الإجرامي الذي يستخدم

في اقترافة الحاسب الآلي كأداة رئيسية. فيما عرَّفها الفقية (ros blat) بأنها كل نشاط غير مشروع موجَّه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي وإلى تحويل طريقه.

وعرفها كلاوس تايدومان بأنها جميع أشكال السلوك غير المشروع الذي يرتكب باسم الحاسب الآلي.

ويرى البعض أن تعريف كلٍّ من (marwe) و(ros blat) جاءا مقتصرين على الإحاطة بأوجة الظاهرة الإجرامية، أما تعريف كلاوس تايدومان فيؤخذ عليه أن بالغ في العمومية والاتساع؛ لأنه يُدخِل فيه كل سلوك غير مشروع أو ضارّ بالمجتمع.

ويدخل فى نطاق تعريفات مفهوم الجريمة المعلوماتية الضيقة، تعريف مكتب تقويم التقنية في الولايات المتحدة الأمريكية، حيث يعرف الجريمة المعلوماتية من خلال تحديد مفهوم جريمة الحاسِب بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً.

## التعريفات الموسّعة لمفهوم الجريمة المعلوماتية

ذهب الفقيهان (michel&credo) إلى أن جريمة الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة، هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرّح به لحاسِب المجنيِّ عليه أو بياناته، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية، سواءٌ على بطاقات الائتمان، وانتهاك ماكينات الحساب الآلي بما تتضمنه من شيكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب، بل وإلى سرقة الحاسب في حد ذاتة وأيٍّ من مكوّناته.

وذهب رأي آخر من الفقة إلى تعريف الجريمة المعلوماتية بأنها عمل أو

امتناع يأتيه الإنسان، إضراراً بمكونات الحاسب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض لها عقاباً.

ويرى جانب من الفقهاء من أنصار هذا الاتجاة الموسّع، بأنها كل سلوك إجرامي يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر.

ويذهب البعض إلى أنه عند وضع تعريف محدد للجريمة المعلوماتية يجب مراعاة عدة اعتبارات مهمة منها :ـ

1 ـ أن يكون هذا التعريف مقبولاً ومفهوماً على المستوى العالمي.

2 ـ أن يراعي هذا التعريف التطور السريع والمتلاحق في تكنولوجيا المعلومات.

3 ـ أن يحدّد التعريف الدور الذي يقوم به جهاز الكمبيوتر في إتمام النشاط الإجرامي.

4 ـ أن يفرّق هذا التعريف بين الجريمة العادية والجريمة المعلوماتية وذلك عن طريق إيضاح الخصائص المميزة للجريمة المعلوماتية.

## موقف بعض التشريعات والهيئات الدولية من تعريف الجريمة المعلوماتية

أشارت الأمم المتحدة في المدونة الصادرة عنها بشأن الجريمة المعلوماتية، إلى الخلاف الواقع بين الخبراء حول ماهية العناصر المكونة لجرائم الكمبيوتر أو حتى المتعلقة بالكمبيوتر، ولعل ذلك ما يفسّر عدم التوصل إلى تعريف متفق علية دولياً لهذه المصطلحات وإن كان هؤلاء قد اتفقوا ضمناً على وجود ظاهرة تتزايد بمعدلات عالمية لتلك الجرائم.

وإن كان مكتب تقويم التقنية في الولايات المتحدة الأمريكية، قد عرف الجريمة المعلوماتية بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج

المعلوماتية دوراً رئيسياً، فإن قانون الكيان الصهيوني(إسرائيل) رقم 5755 لسنة 1995 فى شأن جرائم الحاسب الآلي، قد عرفها بأنها تلك الجرائم التي تشمل العبث ببرامج الكمبيوتر على نحو يعوق استخدامها، أو تحلّ معلومات غير مُصرَّح بها إلا لأشخاص محددين، وكذلك اختراق الكمبيوتر بغرض ارتكاب جريمة أخرى أو بث فيروس من شأنة التأثير على أدائه.

## المفهوم القانوني للمعلومات

تعتبر المعلومات في الوقت الراهن سلعة تُباع وتُشترى ومصدر قوة اقتصادية وسياسية وعسكرية، وذلك لارتباطها بمختلف مجالات النشاط الإنساني وتداخلها في جوانب الحياة العصرية كافة، وبات الوعي بأهميتها مظهراً لتقدم الأمم والشعوب.

وسوف نعرض هنا لماهية المعلومة من حيث تعريفها ثم أنواعها والشروط اللازم توافرها فيها، وطبيعتها القانونية، والمسؤولية عنها.

## تعريف المعلومة

لم تعد المعلومات الآن مجرد نوع من الرفاهية والترف تتباهى به الشعوب أو المنظمات، وإنما أصبحت ركيزة أساسية في تقدم وتطور المجتمع وتحقيق تقدمه ورفاهيته المنشودة،وفى سبيل ذلك وضع عدد غير قليل من التشريعات الوطنية المختلفة تعريفاً للمعلومة وهو ما سوف نعرض للعديد منها.

وقد عرّف المشرع الأمريكي المعلومات في قانون المعاملات التجارية الإلكتروني لعام 1999 بالفقرة العاشرة من المادة الثانية، بأنها تشمل (البيانات والكلمات والصور والأصوات والوسائل وبرامج الكمبيوتر والبرامج المضغوطة والموضوعة على الأقراص المرنة وقواعد البيانات أو ما شابه ذلك.

ونجد أن التعريف السابق قد وسّع من مفهوم المعلومة ووضع تقريباً، كل

ما يتعلق بها، بل أكثر من ذلك، أنه تحسب لما قد يظهر من تطور تكنولوجي جديد.

أما المشرّع الفرنسي ووفقاً للقانون 82 ـ 652 الصادر في 26 يوليو/ تموز لسنة 1982، فيُعرّف المعلومة على أنها صورة أو مستندات أو معطيات أو خطابات أياً كانت طبيعتها.

وأما قانون البحرين رقم 83 لسنة 2002 بشأن المعاملات الإلكترونية، فقد عرّف المعلومات بأنها (البيانات والنصوص والصور والأصوات والرموز وبرامج الحاسوب والبرمجيات ويمكن أن تكون قواعد البيانات والكلام).

كما عرف قانون إمارة دبي بشأن المعاملات والتجارة الإلكترونية رقم 2 لسنة 2002، المعلومات الإلكترونية بأنها (معلومات ذات خصائص إلكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج حاسبٍ أو غيرها من قواعد البيانات).

تلك مجموعة من التشريعات التي وضعت تعريفاً واضحاً للمعلومة والمعلومات كان أغلبها، كما رأينا، يدور حول الأشكال المختلفة للمعلومات وصورها التي تظهر فبها سواءٌ تعلق الأمر برموز أو صور أو بيانات الخ.

وقد ذهب البعض إلى ضرورة التفرقة بين المعلومات والبيانات؛ فالبيانات تعبر عن مجموعة من الأرقام والرموز والحقائق التي لا علاقة بين بعضها البعض، أما المعلومات فهي المعنى الذي يستخلص من هذة البيانات.

## أنواع المعلومات

تقسم المعلومات إلي ثلاث طوائف هي: المعلومات الإسمية، والمعلومات المتعلقة بالمصنفات الفكرية، والمعلومات المباحة.

أما الطائفة الأولى وهى المعلومات الإسمية، فتتقسم إلى مجموعتين هما:

1 ـ المعلومات الموضوعية، وهى تلك المعلومات المرتبطة بشخص المخاطب بها مثل اسمه وموطنه وحالتة الاجتماعية، وهي معلومات لا يجوز الإطلاع عليها إلا بموافقة الشخص نفسه.

2 ـ المعلومات الشخصية، ويقصد بها تلك المعلومات المنسوبة إلى آخر مما يستدعي إدلاء الغير برأيه الشخصي فيها وهي مثل المقالات الصحفية والملفات الإدارية للعاملين لدى جهة معينة.

وأما الطائفة الثانية، وهى المعلومات الخاصة بالمصنفات الفكرية، فهذه المصنفات محمية بموجب قوانين الملكية الفكرية مثل الاختراعات والابتكارات على اختلافها والتسجيلات الفنية والمؤلفات الأدبية.

وأما الطائفة الثالثة وهى المعلومات المباحة، فيقصد بها تلك المعلومات التي يكون مباح للجميع الحصول عليها لأنها بدون مالك، مثل تقارير البورصة والنشرات الجوية؛ هذة المعلومات مباحة للجميع وغير محمية بأي من وسائل الحماية.

## الشروط التي يجب توافرها في المعلومة محلّ الحماية

بصفة عامة، هناك شروط يجب توافرها في المعلومة حتى تتمتع بالحماية القانونية وتتمثل هذه الشروط في الآتي:

### أولاً: أن يتوافر فى المعلومة التحديد والابتكار

المعلومة التي تفتقد لصفة التحديد لا يمكن أن تكون معلومة حقيقية، فإذا كانت المعلومة هي تعبير وصياغة محددة تجعل رسالة ما قابلة للتبليغ عن طريق علامات أو إشارات معينة، وهذا يتطلب أن تكون محددة تحديداً دقيقاً وخصوصاً في مجال الاعتداء على الأموال فهذه الاعتداءات تتطلب أن يكون هناك شيء محددّ ومبتكر. أما الشيء الشائع فلا يتمتع بأي حماية قانونية.

**ثانياً : أن يتوافر في المعلومة السرية والاستئثار.**

السرية صفة لازمة للمعلومة محل الحماية القانونية، ولا يُتصوَّر في جرائم مثل جرائم السرقة والنصب وخيانة الأمانة إذا انعدم هذا الحصر، وذلك لأن المعلومة العامة الشائعة تكون بمنأى عن أي حيازة، وتكتسب المعلومة وصفها إما بالنظر إلى طبيعتها أو بالنظر إلى إرادة الشخص، أو إلى الأمرين معاً مثل الرقم السري (passwoard).

إذن، حتى تتمتع المعلومة بالحماية القانونية، فلابد أن يتوافر فيها الشرطان السابقان، فإذا فقدتهما أصبحت معلومة غير محمية ولا يملكها أحد وغير قابلة لأن يستأثر بها أي شخص، بل أصبحت عامةً لكل من يريد استخدامها.

## المبحث الثانـي:
## الجرائم الرقمية والمعلوماتية: أسبابها وخصائصها والمجرم المعلوماتى الإلكتـرونى

لا شكّ أن فئات مرتكبي الجريمة المعلوماتية تختلف عن مرتكبي الأفعال الإجرامية التقليدية، لذا من الطبيعي أن نجد الاختلاف نفسه في الأسباب والعوامل التي تدفع لارتكاب الفعل غير المشروع [1]، فضلاً عن ذلك، تتمتع

(1) وتتنوع الجرائم المعلوماتية على النحو التالي :
- إساءة استخدام الإنترنت.
- استخدام برامج حلّ وكشف كلمات المرور.
- نشر برامج حصان طروادة وغيرها من الفيروسات.
- هجمات المخربين.
- الهجمات الاختراقية.
- الانتهاكات الأمنية التي تتضمن حالات إساءة استخدام عن طريق الدخول غير المخول به على النظام : تنبع غالبية الانتهاكات الأمنية من مصادر داخلية، مثال : مستخدمين من داخل المؤسسة يحاولون الوصول إلى بيانات سرية غير مخول لهم الاطلاع عليها.

راجع في ذلك : Dr. Linda volonino.cyber terrorism. Op. cit.

جرائم الكمبيوتر والمعلوماتية بعدد من الخصائص التي تختلف تماماً عن الخصائص التى تتمتع بها الجرائم التقليدية، كما أن الجانى الإلكتروني (أو المجرم الإلكتروني) يختلف أيضاً عن المجرم العادي.

ويأتي في طليعة أسباب الجريمة المعلوماتية، غاية التعلّم والتي تتمثل في استخدام الكمبيوتر والإمكانيات المستحدثة لنظم المعلومات، وهناك أمل الربح وروح الكسب التي كثيراً ما تدفع إلى التعدي على نظم المعلومات، بالإضافة إلى الدوافع الشخصية والمؤثرات الخارجية التي قد تكون سبباً في ارتكاب الجريمة المعلوماتية.

## غـايـة التعلم

يشير الأستاذ ليفي مؤلف كتاب قراصنة الأنظمة HACKERS إلى أخلاقيات هؤلاء القراصنة والتي ترتكز على مبدأين أساسيين :

1 ـ أن الدخول إلى أنظمة الكمبيوتر يمكن أن يعلمك كيف يسير العالم.

2 ـ أن جمع المعلومات يجب أن يكون غير خاضع للقيود.

وبناءً على هذين المبدأين فإن أجهزة الكمبيوتر المعنية ما هي إلا آلات للبحث، والمعلومات بدورها ما هي إلا برامج وأنظمة معلومات.

ومن وجهة نظر هؤلاء القراصنة، فإن جميع المعلومات المفيدة بوجه عام يجب أن تكون غير خاضعة للقيود؛ وبعبارة أخرى أن تتاح حرية نسخها وجعلها تتناسب مع استخدامات الأشخاص.

ويرى هؤلاء القراصنة إغلاق بعض نُظُم المعلومات وعدم السماح بالوصول إلى بعض المعلومات وخصوصاً بعضِ المعلومات السرية التي تخص الأفراد.

ويعلق قراصنة الأنظمة أنهم يرغبون في الوصول إلى مصادر المعلومات والحاسبات الإلكترونية والشبكات بغرض التعلم.

وقد لاحظ كل من «ليفي» و«لاندريس» أن قراصنة الأنظمة لديهم الاهتمام الشديد بأجهزة الكمبيوتر وبالتعلم، ويدخل العديد منهم في أجهزة الكمبيوتر على أنهم محترفون ويختار بعض القراصنة الأنظمة لتعلم المزيد عن كيفية عمل الأنظمة.

ويقول «لانديس» إن هؤلاء القراصنة يرغبون في البقاء مجهولين حتى يتمكنوا من الاستمرار في البقاء داخل الأنظمة لأطول وقت ممكن. ويكرس البعض منهم كل وقته في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية للأنظمة، حيث تتفاوت معرفتهم عن الأنظمة والبرمجة إلى حد بعيد.

وكتب أحد قراصنة الأنظمة يقول : يكتشف قراصنة الأنظمة نقطة ضعف أمنية فيحاولون استغلالها لأنها موجودة بهدف عدم تخريب المعلومات أو سرقتها، أعتقد أن ما نقوم به يشبه قيام شخص باستكشاف أساليب جديدة للحصول على المعلومات من المكتبة فيصبح في غاية الإثارة والانهماك.

وينبغي ألا نستهين بكفاءة الشبكات التي يتعلم من خلالها القراصنة حرفتهم.

وهم يقومون بالفعل بالبحث واكتشاف الأنظمة والعمل من خلال الجماعة وتعليم بعضهم البعض. حيث ذكر أحد قراصنة الأنظمة أنه ينتمي إلى مجموعة بحث مهمتها استخراج كميات كبيرة من المعلومات وتعلم أكبر قدر منها.

ويسعى أعضاء القراصنة إلى التخصص والتعاون في المشاريع البحثية وتقاسم البرامج والأخبار وكتابة المقالات وتعريف الآخرين بمجالات اختصاصهم ويبتدع قراصنة الأنظمة نظاماً خاصاً لمجال المعرفة الذي يجذبهم

ويعلمهم التفكير ويسمح لهم بتطبيق ما تعلموه في أنشطة هادفة وإن لم تكن قانونية دائمة[1].

## السعي إلى الربح

أشارت إحدى المجلات المتخصصة في الأمن المعلوماتي securite informatique إلى الرغبة في تحقيق الثراء من بين العوامل الأساسية لارتكاب الجريمة المعلوماتية حيث أشارت :

- أن 43٪ من حالات الغش المعلن عنها قد بوشرت من أجل اختلاس الأموال.
- 23٪ من أجل سرقة المعلومات.
- 19٪ أفعال إتلاف.
- 15٪ سرقة وقت الآلة vol detemps machine، أي الاستعمال غير المشروع للحاسب الآلي لأجل تحقيق أغراض شخصية[2].

لذا نجد أن الدافع لارتكاب الجريمة المعلوماتية يمكن أن يكون سببه مجرد سداد الديون المستحقة أو مشاكل عائلية راجعة للمال أو إدمان ألعاب القمار أو المخدرات. . لذا فإن بيع المعلومات المختلسة هو نشاط متسع للغاية ويمكن أن نبين في هذا المجال واقعة استيلاء مبرمج يعمل لدى إحدى الشركات الألمانية على 22 شريطاً ممغنطاً تحوي معلومات هامة بخصوص عملاء وإنتاج هذه الشركة حيث هدد السارق ببيعها للشركات المنافسة ما لم تدفع له فدية مقدارها 200,000 دولار.

(1) قراصنة أنظمة الكمبيوتر إعداد : دورثي إي. ديننغ، ورقة مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر، واشنطن، ترجمة : آمنة علي يوسف، ديسمبر 1998، ص 8.

(2) G. Delmare, securité informatique Ressource informatique no. 1. Juill 1984.

وبعد أن قامت الشركة بتحليل الموقف وقدرت أن الخسائر التي يمكن أن تنشأ عن إفشاء محتواها تفوق بكثير المبلغ المطلوب فقد فضلت دفع المبلغ من أجل استرداد الشرائط المسروقة[1] .

كذلك أيضاً دفعت الرغبة بمستخدم يعمل في شركة تأمين، كي يحتفظ بوظيفته التي سبق وأن فصل منها، إلى احتجاز الذاكرة المركزية الخاصة بالشركة كرهينة لديه، حيث هدد المختلس رئيسه في العمل بأنه إذا حاول أن يلغي بطاقة أجرته من ذاكرة الحاسب الآلي فإن هذه الأخيرة سوف تدمر تلقائياً عن طريق ما يعرف بالقنابل المنطقية[2] .

## الإثارة والمتعة والتحدي

يدرك القراصنة شيئاً عن أساسيات الكمبيوتر، وأن هذا الأمر يمكن أن يكون ممتعاً، حيث جاء على لسان أحد القراصنة ما يأتي: كانت القرصنة هي النداء الأخير الذي يبعثه دماغي، فقد كنت أعود إلى البيت بعد يوم مُمِلّ آخر في المدرسة، وأدير تشغيل جهاز الكمبيوتر، وأصبح عضواً في نخبة قراصنة الأنظمة. كان الأمر مختلفاً برمّته حيث لا وجود لعطف الكبار وحيث الحكم هو موهبتك فقط. في البدء كنت أسجل إسمي في لوحة النشرات Bulletin Borard الخاصة حيث يقوم الأشخاص الآخرون الذين يفعلون مثلي بالتردد على هذا الموقع، ثم أتصفح أخبار المجتمع وأتبادل المعلومات مع الآخرين في جميع أنحاء البلاد.

وبعد ذلك أبدأ عملية القرصنة الفعلية، وخلال ساعة واحدة يبدأ عقلي بقطع مليون ميل في الساعة وأنسى جسدي تماماً بينما أتنقل من جهاز كمبيوتر

(1) Le Monde informatique 21 fev 1983, Etude la delinquance en col blanc se parte bien

(2) Les escrocs a l'informatique in le Nouvel Economiste no. 202 du 1-10-1979.

إلى آخر محاولاً العثور على سبيل للوصول إلى هدفي. لقد كان الأمر يشبه سرعة العمل في متاهة إلى جانب الاكتشاف الكبير لأعداد ضخمة من المعلومات.

وكان يرافق تزايدُ سرعة الأدرينالين الإثارةَ المحظورةَ بفعل شيء غير قانوني. وكل خطوة أخطوها كان يمكن أن تسقطني بيد السلطات. كنت على حافة التكنولوجيا واكتشاف ما وراءها، واكتشاف الكهوف الإلكترونية التي لم يكن من المفترض وجودي بها[1].

وذكرت Jutian Dibbell بأنها تعتقد بأن المتعة تكمن في المخاطر التي ترتبط بعملية القرصنة، وذكرت قائلة «أن التكنولوجيا تستسلم من الدراما المليئة بالمغامرات وأن قراصنة الأنظمة يعيشون في عالم لا يعتبرون فيه العمل السري سوى لعبة يلهو بها الأطفال.

## الدوافع الشخصية

إن الدافع لارتكاب جرائم الكمبيوتر يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح، ويميل مرتكبو جرائم نظم المعلومات إلى إظهار تفوقهم ومستوى ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبو هذه الجرائم لديهم شغف بالآلة يحاولون إيجاد ـ وغالباً ما يجدون ـ الوسيلة إلى تحطيمها بل والتفوق عليها[2].

---

(1) قراصنة أنظمة الكمبيوتر، إعداد: دروثي إي. دينغ، ورقة مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر، واشنطن، ترجمة: آمنة علي يوسف، ديسمبر 1998 ص 11.

(2) يميل القراصنة إلى التحدي وإلى معرفة تفاصيل تكنولوجيا الكمبيوتر ويبدو أن ولعهم بالكمبيوتر يدفعهم إلى ارتكاب الجرائم وفي هذا الخصوص يحدثنا الدكتور Perey Black أستاذ علم النفس بجامعة نيويورك أن القراصنة يتملكهم جميعاً شعور بالبحث عن القوة ويؤدي ارتكابهم للجرائم بواسطة الكمبيوتر إلى تعويضهم عن الإحساس بالدونية.
راجع في ذلك: CYBER CRIME op.cit.p.25.

ويتزايد شيوع هذا الدافع لدى فئات صغار السن من مرتكبي جرائم الكمبيوتر الذين يمضون وقتاً طويلاً أمام حواسبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الكمبيوتر وشبكات المعلومات وإظهار تفوقهم على وسائل التكنولوجيا، الأمر الذي دفع بالعديد من الفقهاء إلى المناداة بعدم مساءلة مرتكبي جرائم الحاسب الآلي الذين يتمثل باعثهم في إظهار تفوقهم، واعتبار أعمالهم غير منطوية على نيات آثمة.

وقد أمكن الكشف في بعض الأحوال عن أن مجرد إظهار شعور جنون العظمة، وهو الدافع لارتكاب فعل الجريمة المعلوماتية. وفي هذا الشأن نجد المحلل أو المبرمج المعلوماتي، وهو مفتاح سر كل نظام، قد ينتابه إحساس بالإهمال أو بالنقص داخل المنشأة التي يعمل فيها[1]. وقد يندفع تحت تأثير الرغبة القوية من أجل تأكيد قدراته الفنية لإدارة المنشأة إلى ارتكاب الجريمة المعلوماتية، ومن ثم يجد ترضية من خلال الإفصاح عن شخصيته أمام العامة[2].

## ضحايا جريمة سرقة المعلومات

تتميز جرائم الحاسب بالصعوبات البالغة في اكتشافها وبالعجز في حالات كثيرة عن إمكان إثباتها في حالة اكتشافها.

ومَردُّ ذلك الأسباب التالية :

أولاً : لا تخلف جرائم الحاسب آثاراً ظاهرة خارجية فهي تنصبُّ على

(1) تمت مقاضاة شركة مورجان ستانلي مَرّتين من قبل الموظفين العاملين فيها بسبب التمييز العنصري حيث كشفت مبادئ الطب الشرعي المستخدمة في مجال جرائم الكمبيوتر عن وجود «نكات عنصرية» يتم توزيعها عبر نظام البريد الإلكتروني الخاص بالشركة.
راجع في ذلك : DR Linda Volonino op.cit.

(2) د. محمد سامي الشواء سبقت الإشارة إليه، ص ص 52 ـ 53.

البيانات والمعلومات المختزنة في نظم المعلومات والبرامج، ما ينفي وجود أي أثر مادي يمكن الاستعانة به في إثباتها، فالجرائم المعلوماتية ينتفي فيها العنف وسفك الدماء، ولا توجد فيها آثار لاقتحام وسرقة الأموال، وإنما هي أرقام ودلالات تتغير أو تمحي من السجلات. ومما يزيد من هذه الصعوبة ارتكابها في الخفاء، وعدم وجود أثر كتابي مما يجري من خلال تنفيذها من عمليات حيث يتم نقل المعلومات بوساطة النبضات الإلكترونية.

ثانياً : يتم ارتكاب جريمة الحاسب عادةً عن بُعد، فلا ينوجد الفاعل في مسرح الجريمة حيث تتباعد المسافات بين الفاعل والنتيجة، وهذه المسافات لا تقف عند حدود الدولة بل تمتد إلى النطاق الإقليمي لدول أخرى، ما يضاعف صعوبة كشفها أو ملاحقتها.

ثالثاً : تبدو أكثر المشاكل جسامةً، لا في مجال صعوبة اكتشاف وإثبات جرائم الحاسب، بل وفي دراسة هذه الظاهرة في مجملها، هي مشكلة امتناع المجني عليهم عن التبليغ عن الجرائم المرتكبة ضد نظام الحاسب وهو ما يعرف بالرقم الأسود chiffrenoir [1] حيث لا يعلم ضحايا هذه الجرائم شيئاً عنها إلا عندما تكون أنظمتهم المعلوماتية هدفاً لفعل الغش، أو حتى عندما يعلمون فهم يفضلون عدم إفشاء الفعل[2].

---

(1) Dr. Francillon, Les crimes inormatiques et d’autres crimes dans le domaine de la technologie informatique en france Rev. int. pén, 1990, vol 64, p. 293.

(2) في إحدى الوقائع الشهيرة تعرض بنك merchant bank city في بريطانيا لنقل 8 مليون جنيه من أحد أرصدته إلى رقم حساب في سويسرا، وقد تم القبض على الفاعل أثناء محاولته سحب المبلغ المذكور ولكن البنك يدل الادعاء على الفاعل قام بدفع مبلغ مليون جنيه له بشرط عدم إعلام الآخرين عن جريمته وشريطة إعلام البنك عن الآلية التي نجح من خلالها باختراق نظام الأمن الخاص بحاسوب البنك الرئيسي.
راجع في ذلك : يونس خالد عرب مصطفى، جرائم الحاسوب، دراسة مقارنة، رسالة ماجستير مقدمة إلى الجامعة الأردنية 1994، ص 72.

## خصائص الجرائم المتصلة بالكمبيوتر والمعلوماتية:

تتميز الجرائم المرتكبة بوساطة الكمبيوتر كأداة أو كهدف للجريمة بالخصائص التالية:

1. **سرعة التنفيذ**: لا يتطلب تنفيذ الجريمة عبر الهاتف الوقت الكبير، وبضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر. وهذا لا يعني أنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة.

2. **التنفيذ عن بعد**: لا تتطلب جرائم الكمبيوتر في أغلبها (إلا جرائم سرقة معدات الكمبيوتر) وجود الفاعل في مكان الجريمة. بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن الفاعل سواءٌ كان من خلال الدخول إلى الشبكة المعنية أو اعترض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب... الخ.

3. **إخفاء الجريمة**: إن الجرائم التي تقع على الكمبيوتر أو بوساطته كجرائم (الإنترنت) جرائم مخفية، إلا انه يمكن أن تلاحظ آثارها، والتخمين بوقوعها.

4. **الجاذبية**: نظراً لما تمثله سوق الكمبيوتر والإنترنت من ثروة كبيرة للمجرمين أو الإجرام المنظم، فقد غدت أكثر جذباً لاستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويل مسارها أو استخدام أرقام البطاقات... الخ.

5. **عابرة للدول**: إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت جعل الانتشار الثقافي وعولمة الثقافة

والجريمة أمراً ممكناً وشائعاً، لا يعترف بالحدود الإقليمية للدول، ولا بالمكان، ولا بالزمان، وأصبحت ساحتها العالم أجمع.

ففي مجتمع المعلومات تذوب الحدود الجغرافية بين الدول، لارتباط العالم بشبكة واحدة، حيث أن أغلب الجرائم المرتكبة عبر شبكة الإنترنت، يكون الجاني فيها في دولة ما والمجني عليه في دولة أخرى،وقد يكون الضرر المترتب عن الجريمة ليس واقعاً على المجني عليه داخل إقليم دولة الجاني، وتعارض المواد المعروضة مع الثقافات المتلقية لها بخاصة إذا كانت تتعارض في الدين والعرف والاجتماعي النظام الأخلاقي والسياسي للدولة.

6. **جرائم ناعمة**: تتطلب الجريمة التقليدية استخدام الأدوات والعنف أحياناً، كما في جرائم الإرهاب والمخدرات، والسرقة والسطو المسلح.إلا أن الجرائم المتصلة بالكمبيوتر تمتاز بأنها جرائم ناعمة لا تتطلب عنفاً؛ فنقل بيانات من كمبيوتر إلى آخر أو السطو الإلكتروني على أرصدة بنك ما، لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن.

7. **صعوبة إثباتها**: تتميز جرائم الإنترنت عن الجرائم التقليدية بأنها صعبة الإثبات، وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي(بصمات، تخريب، شواهد مادية) وسهولة محو الدليل أو تدميره في زمن متناهي القصر، يضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي، وعدم كفاية القوانين القائمة.

8. **التلوث الثقافي**: لا يتوقف تأثير الجرائم المتصلة بالكمبيوتر عند الأثر المادي الناجم عنها وإنما يتعدى ذلك ليهدد نظام القيم والنظام الأخلاقي بخاصة في المجتمعات المحافظة والمغلقة.

9. عالمية الجريمة والنظام العدلي: نظراً لارتباط المجتمع الدولي إلكترونياً،

فقد أصبح مجتمعنا تخيّلياً، ما أدى إلى أن تكون ساحة المجتمع الدولي بدوله ومجتمعاته كافةً مكاناً لارتكاب الجريمة من كل مكان، ممّا تطلّب أن تمارس الدول المتطورة وبخاصة الصناعية على الدول النامية من أجل سن تشريعات جديدة لمكافحة الجرائم المتصلة بالكمبيوتر، مما استدعى أن تكون القوانين ذات صبغة عالمية.

10. لا يتمّ ـ في الغالب الأعمّ ـ الإبلاغ عن جرائم الإنترنت إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير. لذا نجد أن معظم جرائم الإنترنت تم اكتشافها بالمصادفة ؛ بل وبعد وقت طويل من ارتكابها، زِدّ على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها. فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة ؛ والعدد الذي تم اكتشافه ؛ هو رقم خطير. فالفجوة بين عدد هذه الجرائم الحقيقي ؛ وما تم اكتشافه : فجوة كبيرة.

11. من الناحية النظرية يسهل ارتكاب الجريمة ذات الطابع التقني ؛ كما أنه من السهل إخفاء معالم الجريمة وصعوبة تتبع مرتكبيها.

12. لذا فهذه الجرائم لا تترك أثراً لها بعد ارتكابها ؛ علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت. فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات، ولذا فإن معظم جرائم الإنترنت تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها.

13. تعتمد هذه الجرائم على الذكاء الخارق في ارتكابها ؛ ويصعب على المحقق التقليدي التعامل مع هذه الجرائم. إذ يصعب عليه متابعة جرائم الإنترنت والكشف عنها وإقامة الدليل عليها. فهي جرائم تتسم بالغموض؛ وإثباتها بالصعوبة بمكان والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية.

14. الوصول للحقيقة بشأنها يستوجب الاستعانة بخبرة فنية عالية المستوى.

15. عولمة هذه الجرائم يؤدي إلى تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم؛ والتي هي صورة صادقة من صور العولمة؛ فمن حيث المكان يمكن ارتكاب هذه الجرائم عن بعد، وقد يتعدد هذا المكان بين أكثر من دولة؛ ومن الناحية الزمنية تختلف المواقيت بين الدول؛ الأمر الذي يثير التساؤل حول: تحديد القانون الواجب التطبيق على هذه الجريمة.

16. صعوبة المطالبة بالتعويض المدني بخصوص جرائم الانترنت.

## المجرم المعلوماتي

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز الجريمة المعلوماتية من غيرها من الجرائم التقليدية فحسب، وإنما كان له أثره في تمييز المجرم المعلوماتي من غيره من المجرمين العاديين الذين جنحوا إلى السلوك الإجرامي النمطي. وهذا ما سوف نعرض له موضحين أهم سمات المجرم المعلوماتي ثم خصائصة المميزة وأخيراً لأنماط هذا المجرم وذلك على النحو التالي:

### سمات المجرم المعلوماتي

يمكن أن نستخلص مجموعة من السمات التي يتميز بها المجرم المعلوماتى، والتي يساعد التعرف عليها مواجهة هذا النمط الجديد من المجرمين، ويعد الأستاذ (parker) واحداً من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامه والمجرم المعلوماتي بصفة خاصة، ويرى (parker) أن المجرم المعلوماتي وإن كان يتميز ببعض السمات الخاصة إلا انه في النهاية لا يخرج عن كونة مرتكباً فعلاً إجرامياً يتطلب توقيع العقاب عليه.

وفيما يلي عرض لبعض السمات العديدة للمجرم المعلوماتي والتي في الغالب تميزه عن غيره من المجرمين العاديين:

**أولا: المجرم المعلوماتي، مجرم متخصص**

تبين في عديد من القضايا أن عدداً من المجرمين لا يرتكبون سوى جرائم الكمبيوتر، أي أنهم يتخصصون في هذا النوع من الجرائم، دون أن يكون لهم أي صلة بأي نوع من الجرائم التقليدية الأخرى، ما يعكس أن المجرم الذي يرتكب الإجرام المعلوماتي هو مجرم في الغالب متخصص في هذا النوع من الإجرام.

**ثانياً: المجرم المعلوماتي، مجرم عائد إلى الإجرام**

يعود كثير من مجرمي المعلومات إلى ارتكاب جرائم أخرى في مجال الكمبيوتر انطلاقاً من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وأدت إلى تقديمهم إلى المحاكمة في المرة السابقة، ويؤدي ذلك إلى العودة إلى الإجرام، وقد ينتهي بهم الأمر كذلك في المرة التالية إلى تقديمهم إلى المحاكمة.

**ثالثاً: المجرم المعلوماتي، مجرم محترف**

يتمتع المجرم المعلوماتي باحترافية كبيرة في تنفيذ جرائمة، حيث أنه يرتكب هذه الجرائم عن طريق الكمبيوتر الأمر يقتضى الكثير من الدقة والتخصص والاحترافية في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما في حالة البنوك والمؤسسات العسكرية.

**رابعاً: المجرم المعلوماتي، مجرم غير عنيف**

المجرم المعلوماتى من المجرمين الذين لا يلجأون إلى العنف بتاتاً في

تنفيذ جرائمهم وذلك لأنه ينتمي إلى إجرام ـ الحيلة ـ فهو لا يلجا إلى العنف في ارتكاب جرائمة، وهذا النوع من الجرائم لا يستلزم أي قدراً من العناء للقيام به.

فضلاً عما تقدم، فالمجرم المعلوماتي مجرم ذكي، ويتمتع بالتكيف الاجتماعي، أي لا يناصب أحداً العداء وأيضاً يتمتع بالمهارة والمعرفة وأحياناً كثيرة على درجة عالية من الثقافة.

## خصائص المجرم المعلوماتي

يتميز المجرم المعلوماتى كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين، وهي:

**أولاً: المهارة**

يتطلب تنفيذ الجريمة المعلوماتية قدراً من المهارة يتمتع بها الفاعل، والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في المجال التكنولوجي، أو بمجرد التفاعل الاجتماعي مع الآخرين، وهذة ليست قاعدة في أن يكون المجرم المعلوماتى على هذا القدر من العلم، وهذا ما اثبته الواقع العملي أن جانباً من أنجح مجرمي المعلوماتية، لم يتلقوا المهارة اللازمة لارتكاب هذا النوع من الإجرام.

**ثانياً: المعرفة**

تميز المعرفة مجرمي المعلوماتية، حيث يستطيع المجرم المعلوماتى أن يكوِّن تصوراً كاملاً لجريمته، ويرجع ذلك إلى أن المُصرِّح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة وذلك قبل تنفيذ الجريمة.

**ثالثاً: الوسيلة**

ويُراد بها الإمكانيات التي يحتاجها المجرم المعلوماتى لإتمام جريمتة.

وهذه الوسائل قد تكون، في غالب الأحيان، وسائل بسيطة وسهلٌ الحصول عليها، خصوصاً إذا كان النظام الذي يعمل بة الكمبيوتر من الأنظمة الشائعة، أما إذا كان النظام من الأنظمة غير المألوفة، فتكون هذة الوسائل معقدة وعلى قدر من الصعوبة.

**رابعاً: السلطة**

يقصد بالسلطة، الحقوق والمزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمتة، فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة.

وقد تتمثل هذة السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوى على المعلومات، وأيضاً قد تكون السلطة عبارة عن حق الجاني في الدخول إلى الحاسب الآلي وإجراء المعاملات، كما أن السلطة قد تكون شرعية ومن الممكن أن تكون غير شرعية كما في حالة سرقة شفرة الدخول الخاصة بشخص آخر.

**خامساً: الباعث**

وهو الرغبة في تحقيق الربح المادي بطريقة غير مشروعة ويظل هو الباعث الأول وراء ارتكاب الجريمة المعلوماتية. ويرى البعض أيضاً ما يخالف ذلك، في أن الربح المادي لا يُعدّ هو الباعث في أغلب الأحيان على ارتكاب جرائم المعلوماتية وإنما هناك أمور عديدة أخرى، في الغالب تكون هي الباعث، مثل الانتقام من رب العمل، وأيضاً مجرد الرغبة في قهر نظام الحاسب واختراق حاجزه الأمني.

## الأنماط المختلفة للمجرم المعلوماتى

يقسم مجرمو المعلوماتية (cybr criminals) إلى مجموعة مختلفة من

الطوائف، حيث أسفرت الدراسات في هذا المجال عن وجود عدد من الأنماط المختلفة لمجرمي المعلومات، نرصدها فيما يلى:

**الطائفة الأولى (pranksters):**

وهم الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين دون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم. ومن أمثلة هذة الطائفة صغار مجرمي المعلوماتية.

**الطائفة الثانية (hackers):**

وتضم الأشخاص الذين يستهدفون من الدخول إلى أنظمة الحاسبات الآلية غير مصرح لهم بالدخول إليها، كسر الحواجز الأمنية الموضوعة لهذا الغرض وذلك بهدف اكتساب الخبرة وبدافع الفضول، أو لمجرد إثبات القدرة على اختراق هذة الأنظمة.

**الطائفة الثالثة (malicious hackers):**

وهم أشخاص هدفهم إلحاق خسائر بالمجنيّ عليهم، من دون أن يكون الحصول على مكاسب مالية ضمن هذة الأهداف، ويندرج تحت هذة الطائفة الكثير من مخترعي فيروسات الحاسبات الآلية وموزعيها.

**الطائفة الرابعة (personal problem solvers):**

وهم الطائفة الأكثر شيوعاً من مجرمي المعلوماتية، فهم يقومون بارتكاب جرائم المعلوماتية بحيث يترتب عليها في كثير من الأحيان خسائر كبيرة تلحق بالمجنيّ عليه، ويكون الباعث في هذة الجريمة إيجاد حلول لمشاكل مادية تواجة الجاني لا يستطيع حلها بالطرق العادية.

**الطائفة الخامسة (career criminals):**

وهم مجرمو المعلوماتية الذين يهدفون من وراء نشاطهم الإجرامي تحقيق

ربح مادي بطريق غير مشروع، ويقترب المجرم المعلوماتى من هذة الطائفة في سماتة إلى المجرم التقليدي.

ومن جانب آخر، أكدت بعض الدراسات والأبحاث العلمية على أن فئات المجرمين (أو الجناة) تنحدر من:

1 ـ مستخدمو الحاسب في المنازل.

2 ـ الموظفون الساخطون على منظماتهم.

3 ـ المتسللون، ومنهم الهواة أو العابثون بقصد التسلية.

4 ـ المحترفون الذين يتسللون إلى مواقع مختارة بعناية ويعبثون أو يتلفون النظام أو يسرقون محتوياته، وتقع أغلب جرائم الإنترنت حالياً تحت هذه الفئة بتقسيماتها.

5 ـ العاملون في الجريمة المنظمة.

ويتمتع هؤلاء الجُناة بصفاتٍ أخرى غير متوفرة فى الجناة العاديين نذكر منها:

1 ـ الذين تتراوح أعمارهم عادةً بين 18 إلى 46 سنة، والمتوسط العمري لهم 25 عاماً.

2 ـ المعرفة والقدرة الفنية الهائلة.

3 ـ الحرص الشديد وخشية الضبط وافتضاح الأمر.

4 ـ ارتفاع مستوى الذكاء ومحاولة التخفي.

ومن الجدير بالذكر فى هذا الصدد أن هناك اتفاقاً بين الخبراء والمتخصصين على أن جرائم الإنترنت تمثل تحدياً جديداً في عالم الجريمة، وذلك للأسباب التالية:

- **صعوبة التعرف على هوية الجاني،** فهو لا يترك أثراً لجريمته، وإن وجد فقد لا يدلّ عليه.

- **وجود بعض العقبات في محاكمة الجاني** حال اكتشاف هويته إذا كان من بلد لا يعتبر ما قام به جرماً.
- **اتساع شريحة الجناة لتشمل صغار مستخدمي الإنترنت**، بسبب توفر الوسائل والبرامج المستخدمة في التخريب لصغار مستخدمي الإنترنت، مما يجعل جرائم الإنترنت لا تتطلب خبرة عالية.
- **نقص الوعي بسلبية الاستخدام السيئ للإنترنت**، ما يجعل البعض ينظر للأعمال التخريبية على الإنترنت ـ مثل اختراق المواقع ـ كعملٍ بطولي.

## المبحث الثالث:
## تصنيف الجرائم الرقمية والمعلوماتية والإنترنت

### أولاً: الجرائم المرتكبة أثناء أداء الحاسب لوظائفه العادية

لا يتطلب ارتكاب هذا النوع من الجرائم المساس بالوظائف العادية للحاسب الآلي ولا تعديلاً على البيانات المختزنة بذاكرته، بل يقتصر الأمر على الدخول من جانب البعض إلى مركز نظم المعلومات وأداة إلكترونية تسمح بالتقاط المعلومات أو التنصت عليها من بُعْد.

### ثانياً: الاختراق وانتحال الهوية

من الممكن الاختراق أو انتحال الهوية إما مادياً أو إلكترونياً. فالاختراق المادي يسمح بالدخول في مناطق خاضعة للسيطرة عن طريق بوابات إلكترونية أو آلية. وأسلوب الاختراق الأكثر شيوعاً هو أن يقف شخص غير مسموح له بالدخول أمام البوابة المغلقة حاملاً بين ذراعية متعلقات خاصة بالحاسب الآلي كالشرائط الممغنطة desbandes أو ينتظر حتى يتقدم شخص مسموح له بالدخول ويفتح له الباب فيدخل معه في الوقت نفسه. لذا فإنه يمكن القول بأن الوجود في

صالات الحاسبات الآلية هو أمر حتمي لارتكاب هذه الجرائم[1]. وينطوي الفعل غير المشروع هنا على اطلاع غير مسموح به على المعلومات المختزنة في نظم المعلومات وله صور عديدة.

1 ـ سرقة القائمة وهي عملية مادية بحتة يكتفي فيها السارق بسحب القائمة من الطابعة.

2 ـ الاطلاع على المعلومات، والمقصود بذلك مطالعة المعلومات التي تظهر على شاشة الحاسب الآلي.

3 ـ مجرّد التنصُّت على المعلومات، ويتم ذلك عن طريق استخدام مكبر للصوت[2]والذي يلتقط المعلومات والبيانات.

---

(1) انظر : D. Parker, op. cit., p. 44 et s.

(2) قبل أن يقوم Hacker باقتحام شبكة الحاسب الآلي، يجب عليه استخدام تسهيلات اتصال لكي يرتبط بالشبكة وقد يكون تكاليف الاتصال القانوني مع نظام الكمبيوتر المستهدف معرفة الـ Hackers قد تكون مرتفعة للغاية وقد يكون من الممكن تعقبها. لذا يقوم الـ Hackers بتوظيف أساليب فنية لتجنب هاتين المشكلتين: يقوم الـ Hackers بتوظيف أساليب فنينة يطلق عليها عادة الـ Phreaking ومن تطبيقاتها ما يلي :

1 ـ الاتصال التليفوني عَبْر النغمة: وهو أسلوب نقلي يمكن التلاعب من خلاله في شبكات الاتصالات عن طريق استعمال تردد النغمات، والنغمات يمكن استعمالها لتنشيط وتفعيل رقم تليفون غير متصل بما يتيح القدرة لهذا الشخص لاستكمال هذه الخطوط غير المتصلة كما لو كانت خطوطه الخاصة، إنما الفوائد المترتبة على هذه التقنية تشمل تكلفة المكالمة التليفونية لتي تضاف إلى فاتورة التليفون غير المتصل، علاوة على منع حدود أو متابعة أو تقصي هذه المكالمة.

2 ـ تلاعب Pabx: وهو أسلوب تقني يمكن للشخص بموجبه أن يطلب رقم تليفون pabx (وهو صندوق تحويل معدّ يحتوي على عدد من خطوط التليفون المختلفة). ويتم من خلال توصيل مكالمتهم إلكترونياً لواحد من الخطوط في هذا الـ pabox ثم استعمال هذا الخط للأغراض الخاصة.

3 ـ الاتصال الخارجي بالكمبيوتر : وبموجب هذه الوسيلة يستطيع الشخص أن يتصل برقم تليفون معين يتيح له بدوره فرصة الوصول إلى نظام الكمبيوتر أو الوصول إلى مركز اتصالات يتيح لهم المزايا نفسها الموضحة في الأسلوبين السابقين.

=

ويقصد بانتحال الهوية Iusurpation didentitie سرقة شخصية مستخدم آخر ويتطلب الوصل إلى الحاسب الآلي أو إلى الطرفيات معرفة دقيقة لمستعمل الجهاز.

وإن فحص الهوية يرتكز على مجموعة معلومات متوافقة يستخدمها المستعمل ككلمة السر[1] أو أي جملة خاصة بالمستعمل أو أي خاصية فسيولوجية كالبصمة الرقمية أو ملامح للوجه أو هندسة الكف أو الصوت بالإضافة إلى أي شيء يمتلكه المستعمل كالبطاقة الممغنطة أو المفتاح المعدني.

=

4 ـ Austpac: وهي شبكة اتصالات تشرف عليها هيئة المواصلات الرسمية التي تقدم وصلات معينة بين أنظمة الكمبيوتر، وإن الفواتير الخاصة باستعمال هذا النظام تعتمد على استعمال شبكة التعرف على المستعملين Network User Identieication Cnut ويتكون هذا النظام عادة من سلسلة من 9 أرقام وهي شبيهة من حيث المبدأ برقم الـ PIN.

5 ـ الغش في بطاقات الاعتماد: هذا الأسلوب التقني يتضمن اقتباس تفاصيل بطاقات الاعتماد الخاصة بأحد المشتركين الذي يقوم بدوره بطلب مكالمة تليفونية لصالح الطالب وقيد قيمة المكالمة على بطاقة الاعتماد.

6 ـ الاعتراض المادي: إن عملية الاعتراض المادي لخط تليفوني هي عملية بسيطة وتؤدي إلى الفوائد نفسها مثل الاتصال بالنغمة.

7 ـ الوصلات غير القانونية: وهي عبارة عن تنشيط وتشغيل خدمة غير متصلة بدون علم شركة الاتصالات ثم استعمالها حسب رغبتك عن طريق تليفون عادي بدون أن تتلقي الفاتورة. وهذا النوع من الاعتراض يتميز بأنه دائم ومستمر.

انظر: Franklinclrk, investigating computer crime, Ed. CRC page 50.

(1) بعض كلمات السر يتم وضعها من خلال مدير النظام المعلوماتي والبعض الآخر يتم استخدامه من وحي المستخدمين أنفسهم. وبصرف النظر عن ذلك فإن كلمة السر يجب أن تكون مميزة لكل حساب ويجب تغيير وحذف الحسابات التي ليس لها كلمة سر، وينصح بتجنب استعمال كلمات السر التي يسهل الوصول إليها مثل استعمال الأسماء الأولى والأخيرة وتاريخ الميلاد وأرقام الضمان الاجتماعي أو رقم رخصة القيادة فهذه الكلمات يمكن التنبؤ بها.

كما يعرف القراصنة كلمات السر الأكثر شهرة والتي يميل الناس إلى اختيارها لذا يحظر استخدامها مثل كلمة سر passwred وكلمة ادخل Enter وافتح Open وكمبيوتر Computer ويحذر هذا الاستخدام كلمات السر المرتبطة بالهواية كما يحذر تجنب كلمات السر ذات المقطع الكبير أو تلك المتعلقة بمجموعة حروف أو أرقام.

راجع في ذلك: E. Quarantiello (cybercrime) p. 94.

فلو تمكن أي إنسان من الحصول على هذه المجموعة من المعلومات المتوافقة يصبح قادراً على انتحال شخصية المستعمل. وهناك مثال لشاب ذكي أدعي أنه صحفي في إحدى المجلات واتصل بشركة اتصالات هاتفية مدعياً أنه بصدد نشر مقالة عن النظام المعلوماتي المستخدم في الشركة، فدعته الشركة لزيارة مقرها وقدم له موظفوها عرضاً كاملاً ومفصلاً عن الأجهزة المعلوماتية وتطبيقاتها في الشركة وكانت النتيجة أنه سرق منهم معدات تزيد قيمتها على 10,000,000 عشرة ملايين دولار[1].

وفي حالة أخرى استطاع شخص أن يسرق بطاقات ائتمان ممغنطة لكل منها رقم سري يعرفه صاحبه، حيث اتصل بأصحاب هذه البطاقات مدعياً أنه موظف بالمصرف وأخبرهم أنه قد نُمي إلى علمه أن بطاقاتهم قد سرقت وأنه بحاجة لمعرفة الرقم السري لحمايتهم وتزويدهم ببطاقات جديدة. وهكذا نجح المحتال في الحصول على الأرقام السرية لهذه البطاقات ثم استخدمها في سرقة مبالغ من المال من الموزعات الآلية للنقود[2] des distributeurs . وفي حالة ثالثة أرسل فيها بعض الطلبة مذكرة لكل مستخدمي الطرفيات في جامعتهم ذكروا فيها أن أرقام الاتصال قد تغيرت ومنحوهم أرقاماً جديدة تتصل مباشرة بأجهزة الكمبيوتر الخاص بهم والتي تمت برمجتها مسبقاً بشكل مطابق لأجهزة الجامعة.

وهكذا كان يستخدم المستعمل الرقم السري الخاص به بدون تردد حيث يسجله الطلبة ويعاودون مراسلتهم مرة ثانية طالبين منهم أن يعودوا لاستخدام رقم الاتصال القديم.

ولم تكن تلك سوى لعبة استخدام الطلبة من خلال كلمات السر most de pasdse.

---

(1) انظر : D. Parker, op. cit., p. 65.

(2) المرجع والمكان السابقان.

## ثالثاً: السطو المسلح الإلكتروني

ترتب على ظهور تقنيات بث المعلومات على شبكة اتصالات بُعْدّية telematique إلى نشوء مخاطر جديدة نتيجة للإمكانيات المستحدثة للدخول والاستفسار عن بُعد من مراكز نظم المعلومات، حيث تشكل عمليات بث المعلومات نقطة ضعف هامة في نظم المعلومات وذلك على النحو التالي :

**1 ـ التقاط المعلومات الموجودة ما بين الحاسب الآلي والنهاية الطرفية :**

يتيح هذا الالتقاط عن طريق توصيل خطوط تحويلة un brnchement bretelles de derivaitions والتي ترسل إشارات إلكترونية «ذبذبات إلكترونية مكبرة» تمثل المعلومات المختلسة إلى النهاية الطرفية المتجسسة أو عن طريق مرسل صغير يسمح بنقل المعلومات من بُعْد.

وعلى النقيض عندما تسلك المعلومات الطريق الجوي «كما في حالة البث عن طريق القمر الصناعي» توضع هوائيات مطاردة بالقرب من الهوائيات الاحتياطية والتي تسمح بالتقاط الاشعاعات faisceux واحتجاز مضمونها.

**2 ـ التوصيل المباشر على خط تليفوني wiretape :**

وقد سبق معرفة هذه التقنية في بعض المجالات وتباشر عن طريق وضع مركز تنصُّت unetable decoute يسهل تسجيل كل الاتصالات كما يمكن أن تؤدي هذه الوظيفة ميكروفونات صغيرة.

**3 ـ التقاط الاشعاعات الصادرة عن الجهاز المعلوماتي Electromagnetic pickup**

ويمكن عن طريق هذه التقنية إعادة تكوين خصائص المعلومات التي تتحرك وتنتقل من خلال نظام معلوماتي، ويكفي لإتمام ذلك أن تسجل ثم تحل شفرة الإشعاعات الإلكترومغناطيسية المثبتة عن طريق أجهزة إلكترونية.

وفي الحقيقة تصدر بعض عناصر الأنظمة القوية وعلى وجه الخصوص

الطابعات السريعة les imprimantesrapides أثناء تأدية وظيفتها إشعاعات الكترو مغناطيسية، وقد ثبت أنه بإمكان شاحنة صغيرة مجهزة تجهيزاً خاصاً توقف بمحاذاة مبنى مكتظ بالحاسبات الآلية، أن تلتقط وتسجل هذه الإشعاعات.

ويمكن عن طريق جهاز لفك الرموز أن يطلب من طابعة متصلة بنظيرتها الموجودة في المركز المستهدف النسخ الحرفي لهذه المعلومات نفسها.

ويحضرنا في هذا الخصوص مثال شهير للسطو المسلح الإلكتروني وهو خاص باختلاس أموال عن طريق التقاط أمر بالتحويل مرسل من بنك إلى آخر وقد تمكن المختلس من تزييف الرسالة بالأمر بدفع المبلغ نفسه لحساب فتح باسمه.

**4 ـ التدخل غير المشروع في نظام بواسطة طرفية phone Freak :**

يمكن عن طريق تقنية telematique التدخل في نظام معلوماتي من بُعْد ثم يصبح بعد ذلك نسخ أو تدمير بعض المعلومات شيئاً سهلاً. ويكفي لبلوغ ذلك الحصول على حساب آلي ميكروي ومودم Modem والتزود بكلمة السر أو مفتاح الشفرة المناسب[1].

## رابعاً: جرائم الحاسب من خلال التعدي على وظائفه

وتتعدد أنماط هذه الجرائم على النحو التالي :

**أ ـ تعديل المعطيات بدون إذن من صاحبها :**

أصبح تعديل المعطيات le tripatouillage des donnees تقنية سهلة وآمنة ومألوفة من تقنيات الإجرام المعلوماتي، وهي تتمثل في تعديل المعطيات قبل أو أثناء إدخالها في نظم المعلومات أو في لحظة إخراجها من النظام المعلوماتي.

---

(1) الدكتور محمد سامي الشوا، سبقت الإشارة إليه.

ويمكن إجراء هذه التعديلات عَبْر أي شخص والذي ساهم أو له حق الولوج في عمليات إنشاء وتشفير وتسجيل ونقل، والتحقق من نقل البيانات المخصصة للإدخال في نظم المعلومات، وهناك العديد من الأمثلة التي تنطوي على تزوير أو اختلاس الوثائق واستبدال الشرائط الممغنطة[1] أو البطاقات المثقوبة أو أفعال تحطيم إدخال البيانات أو إحداث ثقوب إضافية في البطاقات المثقوبة أو على العكس سد هذه الثقوب، وأخيراً أفعال التحييد أو إلغاء المراقبات اليدوية[2].

وأجريت في انجلترا ما بين عامي 1983 و 1986 دراسات مسحية قام بها Wong تتعلق بحالات الاحتيال في نظم المعلومات حيث تبين من خلالها أن 63٪ من الحالات محل الدراسة قد ارتكبت عن طريق التلاعب في البيانات المدخلة أو في الوثائق الأصلية التي تستمد منها البيانات، وأن أبرز أشكال هذا التلاعب تم عن طريق تحويل المدفوعات من حساب إلى حساب آخر أو بوقف سداد المستحقات أو باصطناع مورِّدين أو عملاء وهميين لهم مستحقات واجبة السداد أو بوضع أسماء زائفة لبعض الموظفين يستحقون أجوراً ومرتبات[3].

---

(1) الشريط الممغنط : وهو شريط مغناطيسي يحوي المعلومات الخاصة بحامل البطاقة بعد تشفيرها بصورة إلكترونية ويمكن قراءة هذه البيانات باستعمال النهاية الطرفية الإلكترونية الموجودة بمقار البنوك ومنافذ البيع.

Document that is being prepared with a view to submission to the Europen Union in Brussels.

(2) انظر في ذلك : D. parker Op. Cit. p. 77

(3) وهكذا استطاع أحد المسؤولين عن نظم المعلومات بإحدى الشركات الفرنسية اختلاس أكثر من مليون فرنك فرنسي عن طريق إعادة ملفات الموظفين السابقين والذين لهم حقوق مالية وقامت بتحويلها إلى حسابه وحسابات أخرى تم افتتاحها خصيصاً لهذا الهدف وبعد ارتكاب الجريمة قام المجرم بمحو آثار كل فعل عن الغش المعلوماتي :

راجع في ذلك : Expertises no. 66 oct. 1984 مشار إليه في : د. محمد سامي الشوا، سبقت الإشارة إليه، ص 73.

ومن تحليل أجراءه معهد ستانفورد الدولي للأبحاث (SRI) بالولايات المتحدة شمل مائة حالة من حالات إساءة استخدام الحاسبات، تبين أن 37,6٪ منها قد ارتكب بإحداث تغيير مباشر direct modification في البيانات المدخلة بينما وقع 9,5٪ منها فقط نتيجة تعديل وتلاعب في البرامج المستخدمة[1].

ومن الحالات الواقعية لجرائم الحاسب الآلي والتي ارتكبت باستخدام هذا الأسلوب ما يأتي :

1 ـ قامت إحدى موظفات أحد فروع بنك ادخار بجنوب ألمانيا بتحويل مبلغ 1,3 مليون مارك ألماني عام 1983 إلى حساب صديقها من خلال إدخال بيانات غير صحيحة إلى حاسوب البنك عبر النهاية الطرفية الموجود بمكتبها.

وقد اكتشفت أنظمة الأمن والرقابة المتطورة التي يستخدمها البنك عدم صحة هذا التحويل في ظهر اليوم ذاته. لكن الإرسال الفوري المباشر (online) للتحويل والسرعة الفائقة في إجراء العمليات المالية عن طريق الأجهزة الإلكترونية الحديثة، أتاح لصديقها بعد بضع دقائق من قيامها بالتحويل، صرف ثلاث شيكات من فرع آخر للبنك بمبلغ 1,28 مليون مارك[2].

2 ـ قام موظف يعمل في مجال معالجة البيانات (قسم الحاسوب) في أحد البنوك السويسرية الكبرى، بالتلاعب في المعاملات المالية الخارجية للمصرف، والاستيلاء مع بعض شركائه على مبالغ طائلة، وكان يمنع، بحكم عمله كمشغل ومراجع بيانات، وصول بعض أوامر تحويل النقود إلى قسم الترميز ebcidubg deoartlebt ليقوم هو بعملية إدخالها إلى الحاسب، غير أنه بدلاً من إدخال القيمة الفعلية لكل أمر تحويل كان

(1) راجع في ذلك الدكتور هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، طبعة 1994، ص 59.

(2) انظر د. هشام رستم، سبقت الإشارة إليه ص 60.

يدخل هذه القيمة مضروبة في ألف، وقد تمكن بهذه الطريقة من الاستيلاء على (700,000) فرنك سويسري من أموال البنك[1].

وهناك حالة ثالثة لموظفة تدعى سارة تعمل في إحدى الشركات وهي مسؤولة عن عملية المراجعة pointage حيث يتمثل هذا العمل في ملْء استمارات كل موظف تثبت فيه عدد ساعات عمله القانونية والإضافية وإسمه ورقمه كما أنها تصحح استمارات الأسبوع السابق وتتأكد من صحة البيانات وتنقل عن طريق آلة التثقيب من الاستمارة إلى البطاقة المثقوبة ثم يقوم بعد ذلك الموظفون بجمع هذه البطاقات المثقوبة حيث يتم حصرها وجمع عدد الساعات عن طريق آلة حاسبة.

ويتم تثقيب عدد من البطاقات ويثبت مجموع الساعات على كل بطاقة ثم تنقل البطاقات بعد ذلك إلى مركز الحاسب الآلي لمعالجتها حيث يقوم هذا الأخير بتنفيذ برنامج الساعات الإضافية والأجور في نهاية كل أسبوع وتطبع الشيكات في الأسبوع التالي.

وكانت سارة شغوفة لمعرفة أسلوب عمل كل جهاز وليس عملها فقط كما كانت رأسها مليئة بالأفكار الجريئة وعينها تراقب العملية اليدوية فأيقنت أن كل المراجعات وتصحيح المعطيات تقوم على أساس واحد هو اسم الموظف كما لاحظت أن أرقام الهوية المدونة على الاستمارة لا تستخدم أبداً.

وبدأت سارة القيام بأولى محاولاتها الفردية فوضعت اسم موظف ورقم موظف آخر على استمارة وانتظرت لتعرف النتيجة، حيث تلقت تقريراً مطبوعاً على الكمبيوتر يخبرها بوجود حالة شاذة؛ فقد ذكر الكمبيوتر أن الموظف الذي سجلت رقمه عمل 80 ساعة قانونية أي ضعف الحد الأقصى لساعات العمل وعلى ما يبدو فقد كشف نظام الكمبيوتر الخطأ على أساس أن أحداً لا يستطيع

(1) المرجع والمكان السابقان.

أن يعمل أكثر من 40 ساعة ثم تساءلت سارة عما قد يحدث لو استخدمت أسماء الموظفين الذين عادة ما يعملون عدة ساعات إضافية وسجلت مع أسمائهم أرقامها هي، ثم سجلت عدة ساعات إضافية على استمارات إضافية حيث توقعت أن يسجل لها الكمبيوتر هذه الساعات الإضافية طالما أن رقمها هو المدون على الاستمارة. وبدأت التنفيذ واحدة وعدد من الساعات وانتظرت الأسبوع الآتي حيث موعد صرف الشيكات. وفي يوم الجمعة فتحت مظروف مرتبها ووجدت أجر الساعات الإضافية التي لم تعملها مضافا إلى مرتبها. ولم تحاول سارة أن تبلغ الإدارة عن هذا الخطأ وانتهزت فرصة المال السهل واستطاعت أن تحصل على عدة آلاف من الدولارات كل عام. وأثناء قيام أحد مفتشي الإدارة بتصفح استمارات الدخل السنوي للموظفين تعجب من ارتفاع راتب سارة بهذا الشكل الملحوظ، فبدأ فضوله يدفعه بطرح العديد من الأسئلة وإلى مراقبة السجلات وتأكد من عملية التحايل ثم اعترفت سارة بهدوء أمام المفتش بهذا العمل غير المشروع حيث ذكرت في البداية أنها كانت سعيدة للمخاطرة لكن الموضوع تحول بعد ذلك إلى روتين ثم إلى قلق في الشهور الأخيرة.

وأعادت سارة للإدارة المبالغ التي حصلت عليها في السنة الأخيرة وبدا عليها الندم وهي تصف عملية التحايل بالتفصيل.

وشعر المفتش الإداري بخيبة الأمل وهو يستمع إلى مدى بساطة أسلوب سارة وبدأ يفكر في ضرورة إصلاح الخطأ وتعديل البرامج تعديلاً جوهرياً، ولكن وجد أن ذلك يحتاج إلى مبالغ باهظة، وفي النهاية اضطر لتأجيل عملية الإصلاح بأكملها. والغريب أن سارة حصلت على ترقية ومرتب أعلى بعد أن وعدت بعدم كشف الأسلوب الذي اتبعته في السرقة[1].

(1) راجع في ذلك : D. Parker op. cit. p. 81

**ب ـ تقنية Superzapping :**

يطلق مصطلح Superzapping على تقنية الاستخدام بأسلوب غير شرعي للبرامج الخدمية التي تؤثر على المعطيات المحفوظة في جهاز الكمبيوتر أو في ذاكرته، وهذا التأثير قد يكون بالتعديل أو الإلغاء أو النسخ أو الإدخال أو الاستعمال أو المنع.

ومصطلح Superzapping مشتق اسمه من Superzap وهو البرنامج الخدمي الذي يستخدم في العديد من مراكز نظم المعلومات كأداة نظام. وأي مركز نظم معلومات بسير وفقاً لخطة عمل ناجحة وفعالة لا بدّ له من برنامج يلجأ إليه عند الحاجة بغرض التعديل أو الكشف عن أي غموض في جهاز الكمبيوتر.

وأحياناً تتوقف أجهزة الكمبيوتر أو لا تعمل بالكفاءة المرجوة ويصبح إصلاحها أو إعادة تشغيلها غير مفيد وأحياناً أخرى يحتاج الكمبيوتر لعملية تعديل لا تسمح بها أساليب الولوج المألوفة. وفي مثل هذه الحالات فإن برامج الولوج الإجمالية تكون ضرورية، حيث يمكن تشبيهها في مثل هذه الأحوال بمفتاح يستخدم في حالات فقد كل المفاتيح الأخرى.

وهذه النوعية من البرامج الخدمية لها القدرة على فعل كل شيء وهي في الوقت نفسه أدوات خطيرة إذا وصلت إلى أيدي أشخاص غير شرفاء، لهذا يجب الحفاظ عليها بعناية ويجب أن توضع بمنأى عن المستخدمين غير الشرعيين. لكننا أحياناً نجدها في مكتبات البرامج، لذا فإن أي شخص سواء كان مبرمِجاً أو مشرفاً فنياً والذي يعرف استخدامها ومكانها فإنه يمكنه الحصول عليها. وهناك مثال على سرعة هذا البرنامج الذي تسبب في خسارة مقدارها 128,000 دولار من أحد البنوك الذي يقع في ولاية نيوجرسي، حيث كان رئيس قسم الاستثمار لهذا البنك يستخدم برنامجاً من نوع Superzap لإجراء بعض التعديلات في الحسابات الراكدة le solde des comptes وتصحيح الأخطاء وفقاً للتوجيهات الممنوحة له من الإدارة حيث لاحظ أن التصحيح لا يتم على أحسن وجه.

وفي أثناء محاولاته أيقن أنه من السهل إجراء التعديلات دون التعرض لأية رقابة ودون ترك أي دليل على قوائم المعطيات، فبدأ يحول مبالغ إلى حسابات ثلاثة من أصدقائه، وهو واثق أن الوسائل التكنولوجية ستعجز عن اكتشاف الاحتيال[1].

### ج ـ تقنية الاسترجاع Recuperation :

وهي عبارة عن تقنية يستخدمها شخص من أجل الحصول على معلومات موجودة في نظام معلوماتي أو قريبة من نظام معلوماتي بعد تنفيذ عمل ما.

ويمكن أن يتمثل الاسترجاع البسيط والمادي في التفتيش في سلال المهملات لأجل الحصول على نسخ من القوائم الملقاة فيها أو العثور على ورقة كربون المستخدم في نسخ تلك القوائم، وتستلزم الأساليب الأكثر تقنية وخداعاً للاسترجاع ضرورة البحث في المعطيات الموجودة داخل الحاسب الآلي بعد تنفيذ عمل ما، وعلى سبيل المثال لا يمكن لنظام التشغيل un systeme d'exploitation أن يمحو مناطق الذاكرة المغلقة les zones de memoiretampn والمستخدمة بوساطة الذاكرة المؤقتة لمعطيات الإدخال أو الخروج.

وهناك بعض أنظمة التشغيل التي لا تمحو مضمون ذاكرة الاسطوانة أو الشريط الممغنط، والسبب في ذلك أن هذا العمل يستغرق وقتاً كبيراً. لذا فإن المعطيات الجديدة يتم كتابتها فوق المعطيات القديمة. ومن ثم يمكن بسهولة قراءة هذه المعطيات القديمة قبل أن تحل محلها المعطيات الجديدة. فإذا ما تم حفظ الذاكرة واستخدمت في عمل سابق ثم أسند إليها عمل جديد، فإن هذا الأخير يمكن من خلاله الولوج إلى الذاكرة نفسها ولا يكتب إلا القليل من المعطيات الموجودة في هذه الذاكرة، ولكن يمكن بعد ذلك أن يعيد قراءة كل

---

(1) راجع : D. Parker, op. cit., p. 85.

محتوى الذاكرة المستولي عليها أو استعادتها، وكذلك البيانات المختزنة بوساطة العمل السابق.

وكان عدد من شركات البترول ـ كعملاء يتبع إدارة المشاركة بالوقت، ولاحظ المسؤول عن قسم تشغيل الحاسب الآلي أنه في كل مرة يستخدم فيها أحد العملاء الخدمات المعلوماتية، فعليه أن يستخدم شريطاً جديداً للعمل، وهذا يؤدي إلى أن القائم على نظام التشغيل يقرأ المعطيات الموجودة على الشريط قبل أن تكتب عليها أي شيء، ولما تكرر هذا الأمر أثار دهشته فرفع الأمر إلى إدارته وبعد تحرياته البسيطة تبين أن العميل كان يقوم بالتجسس الصناعي ويحصل على البيانات من الذاكرة الخاصة لمختلف شركات البترول، وهي بيانات مسجلة على شرائط ثم يقوم ببيع هذه المعطيات الثمينة لشركات بترولية منافسة[1].

**د ـ تقنية Chausse - trapes, techniques du cheval de troie et de salami**

**1 ـ chausse - trapes:**

يقوم المبرمجون في مجال البرامج التطبيقية programmes d'application والتي تقوم بمعالجة البيانات الخاصة بالإدارة وأنظمة التشغيل والتي تنحصر مهمتها في ضمان تشغيل أنظمة المعلومات بإدخال برامج اختبار وإضافة تعليمات تكميلية وأساليب للحصول على نتائج وسيطة، ويمكن تشبيه هذه المساعدات بالسقالات المستخدمة في بناء المساكن. ومن بين أهداف نظام التشغيل مراقبة الولوج إلى النظام المعلوماتي من جهة، وضمان التحكم في استخدامه على نحو دقيق من جهة أخرى. وعلاوة على ذلك فهو لا يسمح لا بالتعديل ولا بإدخال تعليمات إلا باستثناء الحصول على تصريح لازم لمباشرة ذلك، والذي يجب أن يكون على قدر من الدقة ويطبق حرفياً.

(1) Parker, op. cit. p. 86

ومن ثم فإن مبرمجي النظام يدخلون أحياناً أساليب منطقية ومؤقتة كي تسمح لهم بتخطي هذه القيود أثناء مراحل الاختبار وتزايد البرامج، أو في مرحلة تأتي بعد ذلك عند صيانة النظام أو تعديله.

ويتغاضي المبرمجون أحياناً عن أخطاء موجودة في برامجهم، وهذه لا يتم اكتشافها إلا في مرحلة الاختبار، وتصبح بعد ذلك مهملة، وعندئذ يضعون مختصرات، والتي تخترق أساليب تصحيح البرامج وشروط استخدام النظام. وعلى سبيل المثال حينما يقوم برنامج يدعي «X» بالاتصال ببرنامج يدعي «Y» فإن المعطيات اللازمة لبرنامج «Y» فقط هي التي يجب أن تكون على قدر كبير من سهولة الوصول إليها.

وقد تكون الجهود الخاصة بالبرمجة اللازمة لجمع كل البيانات، على قدر من الصعوبة، في حين أن هناك تقنية على قدر كبير من البساطة ولكنها تبرهن على الإهمال، وتتمثل في جعل المعلومات سهلة الوصول إلى البرنامج «Y» حيث ترشده إلى الأماكن الخاصة بالمعطيات والتي تسمح للبرنامج «Y» بالولوج إلى منطقة معطيات قريبة جداً وأكثر من اللازم، وهذا ينطوي على مخالفة مبدأ الامتياز الأقل moindre privilege.

وهو الذي يقلّل من معدل أمان النظام، ويبقي البرامج متزامنة في الذاكرة بحيث يجب أن يصمم على نحو تُحذر إحداها الأخرى كما لو كانت داخل بيئة عدوانية. والخسائر التي يمكن أن يسببها أي برنامج دخيل يجب أن تكون على نحو ضئيل.

ويمكن أيضاً لمصممي البرامج الضخمة التدخل في حالة السهو ومواطن الضعف وبسبب أوجه القصور على مستوى البرنامج أيضاً.

وعلى سبيل المثال؛ من المألوف بصفة دورية عمل نسخ احتياطية تكميلية لمحتويات وحدة الذاكرة الأولية doit etre maintenuou vameliore وذلك أثناء

تنفيذ الأعمال الممتدة للإنتاج، وتخزن هذه النسخة على وحدة ذاكرة ثانوية (وهي عبارة عن شريط ممغنط أو إسطوانة) وذلك من أجل السماح بإعادة تكوين البطاقات وإعادة التشغيل في حالة حدوث أي عطل طارئ، وذلك بهدف تجنب إعادة تنفيذ هذا العمل كلّه. وفي الأنظمة ذات التصميم المتواضع، فإن العلامات يتم نسخها أيضاً، ثم إعادة تكوينها فيما بعد استناداً إلى النسخة الاحتياطية في حالة حدوث عطل، ويمكن أثناء هذه الفترة إعادة تكوين النسخة الاحتياطية بتعديل البيانات الخاصة بمفتاح الشِفرة.

وهكذا، يمكن لبرامج النسخة الاحتياطية أن تكون لها القدرة على الولوج في مناطق أكثر اتساعاً للبيانات. ويمكن أيضاً إحداث أفعال تَعَدٍّ في الدوائر الإلكترونية، وعلى سبيل المثال يمكن لتلك الدوائر أن تنفذ مجموعات متوافقة للتشغيل ولكنها غير متوقعة، ما يعرض النظام للخطر.

ويكتشف المبرمجون المَهَرة ـ عند استخدام وصيانة البرامج والدوائر ـ بعض الفخاخ سواء لأجل تحقيق غايات مفيدة أو لتنفيذ أعمال غير مشروعة[1].

وهناك أمثلة متعددة لاستخدام هذه التقنية ومنها ما يأتي :

**الحالة الأولى** : اكتشف أحد مبرمجي النظم فخاً داخل مصنف Fortran حيث يسمح الفخ للمبرمج الذي يستخدم لغة Fortran في الكتابة، بتحويل التحكم في برنامجه إلى ذاكرة تُستَخدم للبيانات على النحو الذي أدى إلى تنفيذ الكمبيوتر تعليماتٍ تتكون من بيانات يطلبها المبرمج. فأصبح بمقدور هذا الأخير أن يصدر تعليمات سرية تنفذ بشفرة الآلة عن طريق إدخال معطيات محدّدة كلما استخدم برنامج Fortran. وسبق أن تمّ ذلك في إحدى الشركات التجارية للمشاركة بالوقت، حيث استطاع مبرمج نظم، بالتواطؤ مع موظف في تلك الشركة، أن يستخدم الحاسب الآلي لعدد كبير من الساعات مجاناً وبالأسلوب

(1) انظر في ذلك : D. Parker, op. cit. p. 93

السابق ذكره تمكّن من الحصول على معطيات وبرامج تعمل بنظام المشاركة بالوقت.

**الحالة الثانية** : ومن خلالها اكتشف بعض مهندسي السيارات وجود فخ في برامج إحدى الشركات التي تعمل بنظام المشاركة بالوقت في ولاية فلوريدا ما سمح لهم بالحصول على كلمة السر المميزة وأصبح في مقدورهم الحصول على نسخ من البرامج التجارية السرية وشرعوا في استخدامها مجاناً[1].

**2 ـ Cheval De Troie** (حصان طروادة):

إن هذا المصطلح الأسطوري يُضفي طابعاً كلاسيكياً على هذه الوسيلة الإجرامية والتي لم يتم اكتشاف سوى حالات قليلة من هذا النوع من الجرائم، ولكن يكثر الحديث عن هذه التقنية نظراً لنجاحها في غالبية الأحوال، وأن هناك عدداً ضئيلاً من الذين يملكون المهارة والمعرفة لممارسة هذه التقنية، أو لوجود تقنيات إجرامية أسهل وأقل حرفية، مثل تقنية إتلاف المعطيات.

وبرنامج حصان طروادة يتمثل في إدخال أوامر وعلى نحو غير مشروع إلى الحاسب الآلي بهدف تحقيق أغراض إجرامية[2].

**كيفية مباشرة تقنية حصان طروادة :**

يمكن عمل برامج لاستخدام تقنية حصان طروادة[3]، وذلك عن طريق

---

(1) انظر في ذلك : D. Parker, op. cit., p. 94

(2) بدأ هذا البرنامج في الظهور، حسبما يقرر البعض في الولايات المتحدة الأمريكية، في أواخر السبعينات نتيجة لانتشار استخدام اللوحات الإلكترونية للبيانات والتي تتيح بدورها إما تخفيف أو زيادة تحميل البرامج.
راجع في ذلك : د. هشام رستم، سبقت الإشارة إليه ص 71 وما بعدها.

(3) برامج حصان طروادة : وهي تلك البرامج التي تبدو وكأنها قطع جذابة مضافة إلى البرامج، إلا أنها تملك القدرة على الإضرار بالبيانات، وعلى عكس الفيروسات فهي لا تقوم بنسخ نفسها آلياً.
راجع في ذلك : Dr: Linda Volonino Cyber Tevrorism op. cit.

إدخال تعليمات في أحد البرامج أثناء تكوينه، أو بإدخال تعليمات في وقت لاحق في لغة المصدر language source، أو في إدخال تعليمات في لغة الآلة (ولكن هذا يستلزم مجهوداً ضخماً وذلك في المرحلة التي يتم فيها التنفيذ بوساطة الحاسب الآلي).

وعادةً ما تحفظ ترجمة لغة المصدر على شريط أو اسطوانة ممغنطة في مكتبة المصدر، ويتعين استخدام الشريط أو الاسطوانة وكذا برنامج تحديث لإجراء التعديلات والدخول، ومن ثَمّ يمكن الحصول على شريط جديد أو اسطوانة جديدة وإعادة الأصل المستخدم إلى المكتبة. ونسخة حصان طروادة لا تستخدم إلا عندما يكون البرنامج قد انتحل لغة الآلة. وهكذا يحل محل نسخة الإنتاج المستخدمة حتى ذلك الحين.

ولتحويل البرنامج ـ المكتوب بلغة الآلة والمستخدم في الإنتاج ـ إلى حصان طروادة يتوجّب أن يحلّ البرنامج في المكتبة محل برامج الإنتاج والتي عـادة مـا تحفظ على أشـــرطة أو اسـطوانات، وبـدءاً منها يتم مباشـرة تحميل البرامج في الذاكرة. وهناك حل آخر يتمثل في إدخال تعليمات سرية وعلى نحو يجعلها تُعدّ جزءاً من تعديل أو من بطاقات تحديث، تحفظ عادةً على بطاقات مثقوبة أو أشرطة، وهكذا تدخل إلى الحاسب الآلي في كل مرة يستخدم فيها البرنامج.

**إخفاء حصان طروادة:**

يمكن كشف التعديل الدائم أو شبه الدائم للبرنامج، إذا ما تمّ فحص البرنامج يدوياً، أو إذا استُخدم الحاسب الآلي لعمل مقارنة آلية مع النسخة الأصلية.

ولأجل تجنب هذا الكشف، هناك تقنية على قدر كبير من الصعوبة وتتمثل

في إدخال تعليمات سرية وربما أدمجت في برنامج آخر والذي دائماً ما يستخدم أثناء عمل برنامج الإنتاج في الذاكرة.

ويمكن أن يكون المحتوى في حالة حصان طروادة هذا عبارة عن برنامج نفعي programme utilitaire للاختيار أو للطبع، أو برنامج يستخدم في ترجمة برنامج لغة المصدر إلى لغة الآلة، وعندما يتم تنفيذ المحتوي فإن تعليمات حصان طروادة تُجري تعديلاً أو إدخالاً مؤقتاً لتعليمات عديدة في برنامج الإنتاج، وذلك قبل تنفيذ الجزء المعدّل وإلغاء هذا الجزء بعد ذلك عقب تنفيذه[1].

وعادة ما توجد برامج حصان طروادة في برامج الأعمال، كبرامج معالجة النصوص وبرامج إدارة قواعد البيانات، وغالباً ما تكون مختفية في منتصف البرامج أو في مكان غير مستعمل منه. والبرنامج الذي يتضمنها قد يعمل بطريقة صحيحة لعدة شهور قبل أن تظهر الأوامر غير المتوقعة، وقد تظهر هذه الأوامر وتنفذ مباشرة عند تشغيله.

وسُمّي هذا البرنامج بحصان طروادة للدلالة على خطورته وآثاره المدمرة وقدرته على الخداع[2] والمفاجأة والتضليل مثلما كان حصان طروادة الخشبي

---

(1) ومن قبيل ذلك أن يدس تعليمات في الخفاء في البرامج المستخدمة لإصدار شيكات لمستحقيها بصفة دورية (كأرباب المعاشات مثلاً) وإرسالها إليهم عن طريق البريد وتكون مهمتها تحريف الإخطار الذي يجري إدخاله إلى الحاسب بوفاة مستحق الشيك والذي يترتب عليه وقف إصدار شيكات باسمه في المستقبل لتجعله إخطاراً من مستحق الشيك بتغيير عنوانه مؤقتاً لمدة ثلاثة شهور متتالية، وهكذا يصدر الحاسب خلال هذه الشهور شيكات باسمه ترسل إلى العنوان المؤقت الذي يكون مُعِدُّ هذه التعليمات قد حدده ورتب أمر قيامه بتسلّمه والاستيلاء على قيمته. وبعد انقضاء الشهور الثلاثة تعيد التعليمات المخبأة في البرنامج البيانات التي جري تحريفها إلى أصلها لتكون إخطاراً بوفاة مستحق الشيك وهو ما يجعل اكتشاف أمر هذا التلاعب بالغ الصعوبة.

راجع في ذلك : د. هشام رستم، سبقت الإشارة إليه، ص 72 ـ 73.

(2) راجع في ذلك : د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، 1992، ص 102 ـ 103.

الكبير الذي ضم بداخلة مجموعة من الجنود قد أحكم خداع جيش طروادة وهي تدافع عن أرضها حيال غزو أسبرتا لها وفقاً لما جاء بقصص الحب التي رواها الشاعر الأغريقي القديم هوميروس في ملحمتي الإلياذة والأوديسة[1].

## أمثلة واقعية لتقنية حصان طروادة :

### المثال الأول :

هناك رجل يدعي John Mccloud يبلغ من العمر 30 عاماً وكان يعاني العديد من المشاكل، حيث فقد أولاً عشيقته ثم فقد بعد ذلك مهنته وتراكمت عليه الديون بسبب إدمان القمار، وباءت عدة محاولات للاستثمار من جانبه بالفشل، وكان أمله كبيراً في سداد تلك الديون. وكان Mccloud يعمل كمهندس استشاري ومبرمج في شركة أموال مالية في إحدى مدن الجنوب الأمريكي، حيث عرف الناس الممارسات غير الشرعية في قطاع الأعمال، وقد دفعت هذه العوامل جميعها cloud إلى ارتكاب جريمة معلوماتية لم يستطع تفاديها، حيث كانت الشركة تبيع الأوراق المالية (نوع من الشيكات مقبولة الدفع بوساطة مندوبين يغطون عدداً كبيراً من المدن) وعندما يشتري العميل تلك الأوراق المالية تسجل القيمة المطبوعة عليها وسعرها في حسابات الشركة المدينة، ثم يسدد بها العميل ديونه لشخص آخر ويقوم هذا الأخير بإرساله إذن الصرف للشركة ويتسلم القيمة المدونة عليه. وتستعين الشركة بمحاسب مسؤول عن تلك الأوراق المباعة والمشتراة.

ثم قرر Jimmy Saturn مدير الشركة أن يتخلي عن المحاسب وأن يقتني نظاماً معلوماتياً Datapoint 5500 في أغسطس/آب 1980 حيث أبرم Jimmy عقداً من أجل تطوير البرنامج مع إحدى الشركات المتخصصة في نظم

(1) راجع في ذلك : د. هشام رستم، سبقت الإشارة إليه ص 73 ـ 74.

المعلومات وهنا ظهر Cloud على المسرح، حيث قام ببرمجة نظام التطبيقات لجميع الأوراق المالية في نظام Datapoint 5500 ولكن الشركة استغنت عنه بمجرد الانتهاء من هذا العمل، ثم استعان به Jimmy مرة أخرى من أجل تصحيح بعض الأخطاء الموجودة في البرنامج، وفي هذه اللحظة تفاقمت مشاكل Cloud وعلى وجه الخصوص متاعبه المالية ما جعله يفكر في ارتكاب أفعال الاحتيال. وتنفيذاً لفكرته أدخل Cloud في البرنامج ستّ تعليمات خفية بلغة bacic تتيح له تغذية الحاسب ببيانات عن تعاملات وهمية للشركة لكي تعالج وتخزن تحت رمز «E» لأحد ملفات البرنامج، وبحيث لا تظهر البيانات المُدخَلة والمعالجة تحت هذا الرمز في مستخرجات الحاسب.

ومع أن مدير الشركة كان باستطاعته قراءة هذه التعليمات المضافة وإدراك دلالتها إلا أنه لم يفعل لفرط ثقته في Cloud، بخاصة وأن الأخير كان قد أخطره أنه قد أدخل الرمز «E» في البرنامج ليدرج تحت بيانات وهمية ـ تُمحى فيما بعد ـ بغرض تجربة البرنامج والتأكد من دقة أدائه لمهامه، وهو إجراء يتمّ في العادة اتباعه لاختبار مدى صحة عمل البرامج.

وارتكزت خطة Cloud في اختلاس أموال الشركة على سرقة بطاقات الأمر بدفع النقود وإدخال بيانات إلى الحاسب تحت الرمز «E» ثم تعبئتها ببياناته الشخصية والتوجه إلى البنك بعد ذلك لتحصيلها، وبهذه الطريقة كانت البيانات الخاصة بهذه البطاقات تُدرج، داخل نظام معلومات الحاسب فقط، دون أن يكون لها أي أساس فعلي، ودون أن تظهر في المُستخرَجات المطبوعة للحاسب، ورغم أن هذه البطاقات كانت تحمل أرقاماً متسلسلة، إلا أن سرقتها لم تكن تثير انتباه المراجعين في الشركة لشيوع اعتقاد بينهم بإمكانية فقدها أثناء عملية الانتقال إلى النظام المحاسبي الجديد أو أثناء عمليات تداولها بالبريد.

وتجنباً لظهور عجز في ميزانية الشركة نتيجة الاستيلاء على أموالها، عمد

Cloud إلى تغطية هذا العجز كلما توافر لديه مال، حيث كان يسدد باسم وهمي مالاً للشركة يدخله في نظام حاسبها تحت الرمز «E» بيد أنه لم يتمكن في إحدى المرات من تغطية عجز ظهر بحسابات الشركة فاق مجموعه 100,000 دولار، ما دعا مدير الشركة إلى تكليف المختصة بمراجعة الحسابات بفحص الأمر لاكتشاف مصدر الخطأ المسبب للعجز وتصحيح الحسابات، غير أن الأخيرة تقاعست عن القيام بذلك لمدة ثلاثة شهور، ثم قامت تحت إلحاح مدير الشركة بتحديد يوم معين (7 مايو 1981) لبدء عمليات الفحص والمراجعة.

ولأن عمليات الفحص والمراجعة كان يمكن أن تسفر عن كشف تلاعبه فقط اضطر Cloud إلى اللجوء إلى الوسائل التقليدية لإخفاء معالم جريمته حيث اقتحم ليلاً في اليوم السابق على موعد إجراء الفحص والمراجعة مقر الشركة وقام بسرقة بعض الوثائق المثبتة لإدانته، وكان منطقياً أن يركز البوليس في تحقيقاته، بعد إخطاره بالاقتحام والسرقة صباحاً،على طبيعة المسروقات وأهميتها والدافع وراء سرقتها، وهو ما قاده إلى الاشتباه في Cloud الذي استشعر صعوبة موقفه فبادر إلى الاعتراف بجريمته عند مواجهته[1].

**المثال الثاني :**

لم تُعرف سوى حالة واحدة لإدخال تقنية حصان طروادة إلى الدوائر الإلكترونية، وأول حالة تم التبليغ عنها كانت في نوفمبر 1981 حيث تم القبض على رجلين في وسط السويد يبيعان الزهور في محل صغير، ولم يكن هذا العمل سوى ستار لبيع دوائر مطبوعة بديلة بالدوائر المستخدمة في الآلات التي تقبل النقود الورقية لشراء الوقود.

وأمكن عن طريق تلك الدوائر المطبوعة المقلّدة الحصول على الوقود

(1) انظر في ذلك : D. Parker سبقت الإشارة إليه، ص 100 ـ 101.

مجاناً وانتشرت هذه الحيلة في السويد كلها مما تسبب في إلحاق خسائر جسيمة في محطات الوقود[1].

**هـ ـ تقنية SALAMI:**

وهي إحدى أنماط الجرائم الآلية التي تنطوي على سرقة مبلغ بسيط من المال يتم تحصيله من مصادر متعددة (وهي على منوال أخذ شرائح صغيرة بدون إنقاص الجزء الأكبر بشكل واضح. وعلى سبيل المثال؛ في أحد البنوك حيث يسمح نظام المحاسبة بالإطلاع والتحقق من الحسابات أمكن تغييره (باستخدام أسلوب حصان طروادة لاستقطاع بضعة سنتيمات من عدة حسابات وتحويل هذه المبالغ إلى حساب معيّن، حيث يمكن السحب منه وعلى نحو مشروع. وهكذا لا يوجد اختراق على مستوى أساليب المراقبة لأن النقود لم تسحب على نحو غير مشروع من النظام المحاسبي.

وعلى النقيض، فإن جزءاً صغيراً من المال أعيد توزيعه مرة أخرى بدون قيد أو شرط، ويرتكز نجاح فعل الغش على حقيقة مؤداها أن كل عميل يتحقق من حسابه المفقود إذا كانت النتائج جسيمة أما إذا كانت خسارته ضئيلة فلا يهتم بها.

وقد أطلق على هذه التقنية مصطلح Perruque بسبب استقطاع سنتيم بسنتيم، على نمط الحلاق الذي ينجز عمله شَعرةً بشعرة، وتطبق أحياناً في البنوك والتي تمنح فوائد للحسابات الجارية[2].

ولا تستخدم تقنية SALAMI في قطاعات الأعمال الصغيرة التي لا يوجد فيها عدد كاف من الحسابات. بل إن مجالها المفضل هو القطاعات المصرفية التي تعتمد أعمالها على النظم المعلوماتية، حيث يمكن إدخال تغييرات في

(1) D. Parker، سابق الإشارة إليه ص 101.

(2) انظر في ذلك: B Lussato, le defi informatique ed Fatyard.

البرامج المستخدمة لاقتطاع مبالغ زهيدة القيمة من عدة مئات من الحسابات وتحويل هذه المبالغ إلى حساب خاص للمحتال حيث يقوم بالسحب منه وفقاً للطرق والإجراءات المعتادة[1].

وقد يصل الأمر أحياناً بالمبرمجين من ذوي الميول الإجرامية إلى زرع برنامج فرعي غير مسموح به في البرنامج الأصلي، ومعروف لهم فقط، ويسمح لهم بالولوج غير المشروع في موردات (وهي عبارة عن العناصر الضرورية اللازمة لتشغيل نظم المعلومات) في الحاسب الآلي.

ويمكن وضع هذا البرنامج الصغير السري وبمهارة بين آلاف التعليمات التي تكوّن برنامجاً معلوماتياً.

ومن أمثلة استخدام تقنية Salami ما قام به مبرمج يعمل في أحد البنوك بتعديل برنامج إدارة الحسابات الخاصة بالبنك، بحيث يضيف عشرة سنتات لمصاريف إدارة الحسابات الداخلية على كل عشرة دولارات، ودولار واحد على الحسابات التي تتجاوز عشرة دولارات. وتم تسجيل المصاريف الزائدة في حساب خاص فتحه باسم مستعار Zzwicke.

وهكذا حصل على عدة مئات من الدولارات كل شهر وكان بالإمكان أن يستمر هذا الأمر الإجرامي لولا أن البنك أراد بمناسبة تأسيس شركة جديدة للدعاية أن يكافئ أول وآخر عميل له وفقاً للترتيب الأبجدي للحروف وحينئذ اكتشف عدم وجود ما يسمى Zzwicke [2].

وهناك مثال آخر لموظف أمريكي يدعي E. Royce كان يعمل بإدارة ائتمان

---

(1) راجع في ذلك : D. Parker, op. cit., p. 103.
د. جميل عبد الباقي الصغير - القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناتجة عن استخدام الحاسب الآلي، الطبعة الأولى، 1992، دار النهضة العربية، ص 47.

(2) راجع د. محمد سامي الشوا، سبقت الإشارة إليه ص 78.

في منشأة تجارية ضخمة (تجارة الفواكه والخضار بالجملة) حيث لجأ إلى تقنية Salami لاستقطاع مبالغ زهيدة وعلى فترات زمنية طويلة ومتباينة من خلال الصفقات العديدة التي أبرمتها المنشأة مع المنتجين وموزعي التجزئة. حيث أعد Royce برنامجاً للإدارة المعلوماتية وعلى نحو يسمح بإدارة منتظمة لحسابات المنشأة والتي تتضخم فيه فترات زمنية معينة ببعض الإيرادات ثم يقوم باستقطاع مبلغ زهيد كل شهر من هذه الإيرادات واستطاع Royce أن يحقق فائدة على قدر كبير من الأهمية من خلال هذه المبالغ الزهيدة، وتمكن في خلال ست سنوات من اختلاس مليون واحد من الدولارات[1].

**و ـ القنابل المنطقية : Bombe Logique**

إذا أراد محتال أن يسرق سيارة مصفحة مليئة بالنقود، فهو لن يفعل ذلك يوم الاثنين أو الثلاثاء، ولكن سيختار بالأحرى يوم الجمعة لأن السيارة ستكون عندئذ مليئة بالمال. ويتطابق الموقف في مجال الإجرام المعلوماتي وخصوصاً بالنسبة لأفعال الغش المبرمجة على الحاسبات الآلية ولكن يجب توافر بعض الشروط والتي يمكن اكتشافها بصفة آلية حتى يمكن أن ينجح الاحتيال وعلى نحو مؤكد. ومن هنا تصبح القنبلة المنطقية وسيلة سهلة وجذابة.

والقنبلة المنطقية عبارة عن برنامج أو جزء من برنامج ينفذ في وقت محدد أو على فترات زمنية منتظمة ويتم وضعه داخل النظام المعلوماتي بهدف تحديد ظروف أو حالة محتويات النظام من أجل تسهيل تنفيذ عمل غير مشروع[2].

ويمكن على سبيل المثال إدخال تعليمات في برنامج نظام التشغيل (أي البرنامج الذي يقوم بتحميل ذاكرة الحاسب بالبرامج المراد تنفيذها) وهو الذي

(1) انظر : Linformatique aujourd lui dans le no special monde sep. 1982.

(2) انظر في ذلك : D. Parker, op. cit., p. 110.

ينفذ في كل مرة عملاً جديداً، وينصبّ البحث على عمل معين يمكن أن يكون محلاً للاعتداء، كأن تسعى القنبلة المنطقية إلى البحث عن حرف معين وليكن (حرف الباء) في أي سجل يتضمن أمراً بالدفع وعندما تكتشفه تتحرك متتالية منطقية sequence loghique تعمل على إزالة هذا الحرف من السجل[1].

والقنبلة الزمنية Bombe a retardement على عكس القنبلة المنطقية حيث، تشير إلى حدث في لحظة زمنية محددة بالساعة واليوم والسنة[2]. ويتم إدخالها في برنامج وتنفذ في جزء من الميلي ثانية أو في بضع ثوانٍ أو دقائق وفقاً للتحديد المطلوب. ويمكن على سبيل المثال ضبطها لكي تنفجر بعد عامين في يوم 12 يونيو الساعة الثانية عشرة وخمس وأربعين دقيقة (12,45) عصراً لتحويل مبلغ من المال من حساب شخص معين تلاحظ في اللحظة ذاتها الذي يكون فيها مرتكب الجريمة موجوداً في البرازيل Riod Janeiro.

ومن أمثلة استخدام القنبلة المنطقية ما يلي :

1 ـ قام مبرمج في ألمانيا الديمقراطية (قبل توحيدهما) بزرع برنامج يحوي قنبلة زمنية في النظام المعلوماتى الخاص بالشركة التي يعمل بها، وتم برمجة القنبلة بحيث تنفجر بعد عامين لتركه العمل فيها. وفي حوالى الساعة الثالثة ووفقاً للتاريخ المحدد وكما سجل هذا الأخير في البرنامج، فإن الاستفهام الخاص بيوم وساعة وسند التنفيذ ظل مستمراً، وكان متأكداً من أن لحظة التدمير ستراعى بكل دقة. وبسبب طارئ أدى إلى انهيار النظام المعلوماتي الخاص بالشركة فإن أكثر من 300 طرفية ظلت لا تعمل

(1) انظر في ذلك المرجع والمكان السابقين.

(2) وبعبارة أخرى فالقنابل الزمنية : هي تلك الفيروسات التي تطلق في تاريخ محدد. والقنابل المنطقية هي تلك الفيروسات التي تطلق لشروط محددة.
راجع في ذلك : Cr.Linda Volonino Cyber Terrorism. Op. cit.

لبضعة أيام وكان من الصعب اكتشاف الفاعل نظراً للتفاوت في الزمن بين لحظة ارتكاب الفعل ولحظة تحقيق النتيجة[1].

2 ـ تمكن أحد العاملين بإدارة المياه والطاقة في ولاية لوس انجلوس الأمريكية من وضع قنبلة منطقية في نظام الحاسب الآلي الخاص بها مما أدى إلى تخريب هذا النظام عدة مرات[2].

3 ـ استطاع خبير في نظم المعلومات في الدانمارك من وضع قنبلة منطقية في نظام إحدى الحاسبات الآلية، الأمر الذي ترتب عليه محو أكثر من 100 برنامج. وقد تم أيضاً محو النسخ الاحتياطية عند تشغيلها نظراً لانتقال آثار القنبلة إليه، وتمّ ضبط المجرم وحكم عليه بالحبس لمدة سبعة شهور

**ك ـ فيروس الحب:**

تعاني شبكات الكمبيوتر من الإرهاب عبر الإنترنت بشكل متزايد، وذلك على شكل محاولات متعددة لزرع فيروسات في برامج الكمبيوتر عبر ملحقات البريد الإلكتروني.

ومؤخراً فقد سبب فيروس الحب المدمّر خسائر فادحة لا تزال شركات عديدة تعاني منها، وأسلوب فيروس الحب في الهجوم يعتمد على إرسال رسالة مُغرية شكلاً ومضموناً لحث المتلقين على فتحها.

وفيروس الحب هو نوع من الفيروس المعروف بـ «حصان طروادة» أو دودة البريد الإلكتروني، وستظهر أنواع جديدة من هذا الفيروس قادرة على تهديد ملفات المعلومات الخاصة بالشركات التجارية الكبرى.

---

(1) Hartmann, La criminalité informatique et sa repression par les reformes penales en Allemagne, Droit de l’informatique 1985-6-annex p. 11.

(2) انظر د. هشام رستم، سبقت الإشارة إليه ص 160.

**الطريقة التي يعمل بها فيروس الحب وما شابهه من فيروسات :**

- يصل فيروس الحب على شكل رسالة إلكترونية عادية لها ملحق يسمى «رسالة حُب لك نصّ» هذا في حال تعطيل خاصية الإظهار الكاملة لنهايات الملفات، حيث أن الجزء الأخير من اسم الملف هو «في.بي.إس» وفي هذه الحالة يتنكر الفيروس في شكل رسالة بريدية نصية آمنة تماماً، بينما في الحقيقة تستطيع هذه الرسالة تنفيذ أوامر برمجة كمبيوترية مدمّرة.

بعد فتح الملف المصاب بالفيروس، يقوم الفيروس بتنفيذ خمسه عمليات مدمّرة :

1 ـ يقوم بنسخ نفسه للعديد من الملفات الأخرى، بما يضاعف قدرته على الانتشار.

2 ـ يقوم بتعديل ملف التسجيل الخاص بالكمبيوتر المصاب حتى يمكنه إعادة تنفيذ البرنامج الخاص بالفيروس في كل مرة يتم فيها تشغيل الحاسوب، كما يقوم ايضاً بتشغيل خاصية سرقة كلمة سر من موقع للإنترنت.

3 ـ يقوم بتحديد صفحة قياسية جديدة لبرنامج مايكروسوفت انترنت إكسبلورر.

4 ـ يقوم بإرسال رسالة بريد إلكتروني لكل مستخدمي الكمبيوتر المصاب وكذلك جميع قوائم التوزيع الموجودة في سجل العناوين الإلكترونية الخاص ببرنامج «أوت لوك».

5 ـ يقوم بإصابة سائقات البحث كافة بما في ذلك تلك الخاصة بالشبكة المستخدمة في الشركة والمرتبطة بالجهاز المصاب، ويقوم الفيروس إما بحذف الملفات أو إخفائها ويستبدلها بنسخ منه.

## المبحث الرابع:
## الفيروسات الإلكترونية والرقمية وآليات الوقاية منها

### العوامل المؤثرة في انتشار الفيروسات المعلوماتية[1]

أصبحت شبكة الإنترنت المكان الأمثل لارتكاب جرائم الاحتيال والنهب، بما تتمتع به من تكلفة تركيب منخفضة بالإضافة لإمكانية التعمية الكاملة على الشخصية، وإمكانية الوصول لملايين الضحايا المحتملين عبر أنحاء العالم، فبوسع المجرمين الاختفاء في بلاد بعيدة وانتحال هوية آخرين أو حتى استخدام أدوات ذات تقنية عالية مثل الكتابة المشفرة «الهواتف الخليوية، برامج النشر الصحفي، وبرامج اللوغاريتمات الرياضية التي يمكنها تكوين أرقام عاملة لبطاقات الائتمان».

ويوضح Louis J. freeh مدير مكتب المباحث الفيدرالية الأمريكي أن الإنترنت هي وسط ممتاز لالتقاط الضحايا كما أنها توفر بيئة لا يستطيع فيها الضحايا أن يتحدثوا أو يروا المحتالين، فبوسع أي شخص يحتمي بخصوصية جدران منزله أن يخلق وسيلة احتيال شديدة القناع عبر الإنترنت.

أما Arthur Levitt رئيس قسم مكافحة الجرائم الإلكترونية «سك» فيقول: يمكن بنقرة ماوس إيصال رسالة بريد إلكتروني جماعية غير مخصصة (spam) للمستثمرين بطريقة أسهل وأرخص من تلك المكالمات الباردة التى تجرى بشكل تقليدي، كما أن استخدام الوسيلة الإلكترونية يضفي مسحة من المصداقية على ما يستخدمه المحتال من أدوات حيث بإمكان أي شخص يمتلك جهاز كمبيوتر

---

(1) راجع في ذلك : REPIRT 5
- The first conference on computer forensics & Digital Discovery Tools & Techniques October 21st - 23rd, 2000.

منزلي ومعرفة بنظم الرسم الإلكتروني (graphies) أن يصمم موقعاً جذاباً ـ على أقصى درجة من الحرفية ـ يضاهي موقع شركة «فورشت 500» على الإنترنت. وفي الوقت نفسه يقف تطبيق القانون عاجزاً نتيجة لميراث ثقيل من القوانين الصادرة في عهد ما قبل الإنترنت، تلك القوانين التي تضع قيوداً على عملية التحري والحدود الجغرافية لسلطة الضبط القضائي.

وحتى الآن فقد تم ضبط القليل من محتالي الإنترنت بينما يخضع عدد أقل منهم لعقوبات شديدة، ويضع وصول الإنترنت لجميع أنحاء الكوكب مؤسسات تطبيق القانون المحلية في حرج، نظراً لأنها أنشئت لحماية الحدود الجغرافية للمدينة أو للمقاطعة أو الدولة، من دون أن يكون لديها لا الإمكانات ولا الخبرات التي تمكنها من مواجهة الجرائم المعقدة للاحتيال عبر الإنترنت.

وتعاني الوكالات القومية المتخصصة في مواجهة جرائم الاحتيال الإلكتروني من الإحباط نتيجة الميراث الثقيل من التشريعات التي سُنّت قبل عهد الإنترنت، ومن أشهر هذه الوكالات الشرطة السرية لوزارة الخزانة، والمفوضية التجارية الفيدرالية (إف. تي. سي) .F.T.C، وقسم التفتيش البريدي الأمريكي (يو، أس، بي، اس) .U.S.B.S ومكتب المباحث الفيدرالية الأمريكي، وقسم مكافحة الجرائم الإلكترونية (سك) Securities & Exchange Commission، ويعود هذا الإحباط إلى القيود المفروضة على عمليات التحقيق والحدود الجغرافية لسلطة التحقيق، وعلى سبيل المثال، فقد تشابكت خطوط التحقيق بقضية نَصْبٍ إلكتروني كبري حينما مارس محتالو الإنترنت ـ الذين استهدفوا نشاطات تجارية أمريكية كبير ـ نشاطاتهم من خارج الحدود.

ففي هذه الحالة من المحتمل أن يكونوا بمنأى عن الملاحقة القضائية حيث أنهم لا ينتهكون أي قوانين، فلا وجود لأي قوانين معمول بها حيث يعملون.

وبوسع سلطات الجمارك الأمريكية ـ بما تتمتع به من سلطة الضبطية

القضائية على نطاق قومي ـ أن توضح عدداً من الحالات الناجحة للتنسيق مع سلطات الضبطية القضائية لدول أخرى.

ففي إحدى الحالات تم تنظيم غارات متزامنة في اثنتي عشرة دولة تضم الولايات المتحدة و10 دول من أوروبا الغربية بالإضافة لأستراليا، ومع ذلك يعترف Raymond W. Kelly المفوض العام لمفوضية الجمارك الأمريكية، أنه لا يوجد سوى إجماع ضئيل على مستوى دول الكوكب حول ما هي الأنشطة التي يمكن وصفها بـ «الإجرامية» وتلك التي لا تنطبق عليها هذه الصفة.

- انعقد في مايو 2000 أول مؤتمر لـ «مجموعة الثمانية» حول المسائل المتعلقة بجرائم الإنترنت، فيما لا تزال الخطوط العامة لسياسة الاتحاد الأوروبي حول الجرائم الإلكترونية في طور الإعداد.
- القبض على المحتال ومع ذلك فلا عقوبة.

قد ينأى المحققون بأنفسهم عن إقامة الدعوى في قضايا الاحتيال المالي المعقدة في ظل نظام جنائي يميل لمقاضاة مجرمي الشوارع، حيث أن المحققين ليست لديهم المصادر التي تمكنهم من بناء دعوى يمكن لهيئة المحلفين متابعتها، أو أن المبالغ الخاصة بالقضية قليلة جداً، أو لقلة العدد بقائمة الضحايا.

ويدرك العديد من المحتالين الحدود المالية التي تستلزم تدخلاً من سلطات فرض القانون، لذا يُبقون حدود عمليات احتيالهم دون هذه الحدود، وطبقاً لجريدة «نيويورك تايمز» فإنه بينما وصلت نسبة القبض على مرتكبي الجرائم من ذوي الياقات البيضاء إلى ذروة معدلاتها منذ خمسة أعوام مضت، فإن نسبة الجرائم التي يرتكبها ذوو الياقات البيضاء قد ارتفعت (في النظم الاقتصادية القديمة والحديثة) بنسبة تتراوح بين 10٪ و20٪ خلال الأعوام الخمسة الأخيرة. ويحتج Skolook، المفوض العام لشركة «إنديانا» للمستندات المالية ورئيس اتحاد المتعاملين في السندات المالية بأمريكا الشمالية (إن ـ إي ـ إس ـ

إي ـ إي) .N.A.S.A.A على أن جرائم ذوي الياقات البيضاء لا ينظر إليها بشكل جدي نظراً لكونها معقمة وتخلو من سفك الدماء، ولكونها جرائم فنية. فإذا ما تم القبض على محتالي المستندات المالية، فإنهم يواجهون تهماً إدارية أو مدنية وليس الملاحقة الجنائية. ويضيف Skolook الملاحظة التالية: إذا سرق أحدهم سيارتك فسوف يلقى به في السجن، أما إذا سرق محتال ـ إلكترونياً ـ أموال والديك التي يحتاجان إليها عند تقاعدهما عن العمل، فربما يدفع غرامة فعلته، وهذا ليس عدلاً.

يعتقد الكثير من النقاد، يؤيدهم في ذلك مطبّقو القانون، أنه على الرغم من زيادة الإجراءات الأمنية الجديدة لمواجهة جرائم الإنترنت، فإن المجرمين سيتمكنون من زيادة حجم جرائمهم ذات المستوى التقني المرتفع لفترة من الزمن.

وقد تمثل أحد ردود الأفعال على موجة الجرائم الرقمية في جعل مشاركة المعلومات والتعاون بين الشركات يتم بشكل رسمي وبهذا يمكن التأكد من هذه المعلومات. فعلى سبيل المثال؛ تطبق .F.T.C سياسة فترة تطبيق القانون على التجول عبر الشبكة، وخلال تلك الأيام تنسق الوكالات الفيدرالية فيما بينها عملية مراقبة الشبكة.

ويشكِّل مركز حماية البنية الأساسية القومي .N.J.B.C الذي أنشئ عام 1998 للكشف عن مواجهة الهجمات الإلكترونية على البنية التحتية القومية الحيوية ومركز .I.F.C.C الجديد والذي بدأ نشاطه في ذلك الربيع لجمع وتحليل الاستخبارات الخاصة بجرائم الاحتيال عبر الإنترنت، أمثلةً على التسهيلات المقدمة مِنْ وبين مختلف الوكالات العاملة تحت حماية مكتب المباحث الفيدرالي الأمريكي، كما تبذل جهود متناسقة لتغيير القوانين التي تشكل عائقاً لملاحقة مجرمي الإنترنت. لذا تعمل وزارة العدل على إصدار تشريعات جديدة لتحديث القوانين التي تحكم عمليات التحري والإدعاء في مجال جرائم الإنترنت. ويعلق مدير مكتب المباحث الأمريكية الفيدرالية السيد Freeh قائلاً:

لقد تطورت مشكلة جرائم الإنترنت بشكل سريع أَعجزَ القوانين القائمة عن ملاحقة التغير التقني. ومن بين الأمثلة التي أوردها تحت القوانين المعمول بها حالياً، فإن المحكمة الفيدرالية تستطيع إصدار الأمر بتتبع الاتصالات المُجْراة فقط داخل منطقة عملها وذلك لتزويد سلطات تطبيق القانون بمعلومات المراقبة. ولا نحتاج هنا للقول بأن عملية تتبع اتصال واحد قد يكون مضيعة للوقت والموارد، وبهذه الطريقة تتم عملية إعاقة أو إطالة أمد التحقيقات في مثل هذه الحالات التي تتصل فيها سلطات فرض القانون بمقدِّم خدمة الاتصالات بعد أن يكون قد تخلص من المعلومات الضرورية للتحقيق.

## حدود تطبيق القانون:

بالطبع، هناك العديد من نقاط الاستفهام حول تطبيق القانون الموضوع لحماية الحقوق الدستورية للأفراد. فالمدافعون عن حقوق الفرد الساعون لرؤية هذه الحقوق مطبقة في الحقبة الإلكترونية، يخرجون باعتراضات جديدة لبعض المحاولات لتوسيع السلطات الشُرطية في مجال الإنترنت.

فعلى سبيل المثال؛ إن مركز المعلومات الإلكترونية الخصوصية (إيبك) واتحاد الحدود فوق المدينة الأمريكية .A.C.L.U ومنظمة الحدود الإلكترونية .E.F.F قد رفعوا دعوى بالمحكمة في نوفمبر 1999 لمنع تنفيذ القواعد الفيدرالية الجديدة في مجال الاتصالات .F.C.C، حيث أن هذه القواعد ستمكن مكتب المباحث الفيدرالية الأمريكي من فرض تصميم البنية الأساسية لنظام الاتصالات القومي؛ فطبقاً لقانون مساعدة نظم الاتصالات لتطبيق القانون (كاليا) والذي سُنّ عام 1994، يتعين على شركات الاتصالات تصميم أنظمتها بما يتوافق مع المستويات الفنية للمباحث الفيدرالية الأمريكية وذلك لتسهيل عمليات المراقبة الإلكترونية. ولكن يدفع المعارضون بأن أحكام القواعد الفيدرالية الجديدة في مجال الاتصالات .F.C.C تعطي وكالات فرض القانون سلطات أكبر من تلك التي منحها لهم الكونجرس. ولم تقف جماعات الحقوق الشخصية بمفردها في

هذه المعركة، فقد رفع اتحاد الاتصالات واتحاد صناعة الهواتف الخلوية قضايا مماثلة لنقض أحكام القواعد الفيدرالية الجديدة في مجال الاتصالات F.C.C. وقانون مساعدة نظم الاتصالات لتطبيق القانون (كاليا).

لا يستطيع القطاع الخاص الاعتماد بصورة كلية على تطبيق مواد القانون لحماية مصالحه على الجبهة الرقمية، وعلى الرغم من أن وسائل تطبيق القانون تكتسب أدوات جديدة تمكنها من حراسة الفضاء الإلكتروني فإن العملية تستلزم مجالاً عميقاً وطويل الأمد حول أفضل الطرق لإزالة العوائق التي تخدم أساساً المجرمين، بينما تضع قيوداً ثقيلة على سلطة الحكومة على التدخل في الحياة الشخصية للأفراد. وكما قال William M. Daley وزير التجارة الأمريكي؛ تحشُّد من خبراء تكنولوجيا المعلومات اجتمع هذا الربيع «هذه هي أول مرة في التاريخ الأمريكي لا تستطيع الحكومة بمفردها حماية البنية الأساسية للدولة، فلا نستطيع تأمين قوة شرطية كبيرة بما فيه الكفاية لحماية أصول المعلومات الرئيسية لصناعتنا كافةً، بل لن ترغبوا أنتم في أن نقوم بذلك».

## أساليب الوقاية من الفيروسات المعلوماتية

تتعدد أساليب الوقاية من الفيروسات المعلوماتية، وذلك على النحو التالي:

### أولاً: الاحتياطات العامة لمواجهة الفيروسات المعلوماتية[1]:

يجب تحميل برنامج مضاد للفيروسات داخل الأنظمة المعرضة لخطر الإصابة بها كافة، ويمكن الأخذ بالاحتياطات التالية للحد من سرقة انتشار الفيروسات:

---

(1) راجع في ذلك: Dr: Linda Volonino Cyber Jerrorism op. cit.

1 ـ أن يتم إدخال البرامج المحملة عن طريق الإنترنت من المواقع الموثوق فيها فقط.

2 ـ ألاّ يتم استخدام أي من الأقراص المرنة داخل الكمبيوتر ما لم يُجْرَ عليه فحص دقيق للتأكد من خلوه من الفيروسات.

3 ـ وقف عمل وحدة (الماكرو) كلما أمكن ذلك.

4 ـ يمكن تطعيم الأقراص المرنة ضد الفيروسات التي تصيب قطاع التحميل.

5 ـ الإبقاء على شريط الحماية الموجود في البرامج الجديدة المسجلة على الأقراص المرنة.

6 ـ يجب على مهندسي الكمبيوتر الذين ينتقلون من شبكة إلى أخرى كفالة حماية الأقراص المرنة التي يستخدمونها.

**ثانياً : بعض الاحتياطات الخاصة لمواجهة الفيروسات المعلوماتية**

**1 ـ برنامج كمبيوتر يقضي على فيروسات الماكرو والفيروسات الخاصة بلغة لنص الحساس في البريد الإلكتروني :**

أطلقت شركة «جي.إف.آي.» .J.F.I اليوم برنامجها الرئيسي لحماية البريد الإلكتروني تحت اسم «ميل اسسنشيالز اكستينج إس أم تي بي 3,5» وهو برنامج لفحص محتوى الرسائل الإلكترونية بالإضافة لكونه برنامج مضاد للفيروسات، ويمكن لهذا البرنامج حالياً أن يحمي أجهزة تخزين وإرسال البريد الإلكتروني (الأجهزة الخادمة) ضد جميع فيروسات الماكرو (الماكرو هو مجموعة أوامر تنفيذية فرعية داخل برنامج آخر)، وفيروسات لغة النص الحساس في البريد الإلكتروني حالياً ومستقبلاً. ويعزز هذا الأسلوب من تأمين أجهزة تخزين وإرسال البريد الإلكتروني الرئيسية (الأجهزة الخادمة) مع التأكد من حماية المستخدمين ضد كافة الفيروسات المستقبلية للماكرو ولغة النص

الحساس في البريد الإلكتروني، حتى قبل أن يصدر منتجو برامج محاربة الفيروسات أي تحديث لقائمة فيروسات برامجهم.

وقد صرح السيد/ جاليا ـ منتج هذا البرنامج ـ بأن برنامج ميل اسنشيالز 3,5 يوفر حماية شاملة لبرامج البريد الإلكتروني، حيث بإمكانه حالياً محو أي ماكرو وأي كتابة بلغة النص الحساس من برنامج «ورد» بطريقة آلية، فإذا ما وجد هذا البرنامج أي نص ملحق يحتوي على ماكرو، فإنه يقوم آلياً بمحو الماكرو فوراً، وسيتم إرسال الوثيقة للمرسَل إليه بدون هذا الماكرو الخطير، وبهذا يتم تأمين الوثيقة كلياً. كما أوضح أيضاً أن الفيروسات سيئة السمعة، مثل «ميليسا» الذي انطلق العام الماضي، وفيروس «ريزومي الذي انطلق هذا العام 2000 يعتبران مثالين شهيرين على فيروسات الماكرو. كما أوضح السيد/ جاليا أيضاً أن دخول لغة النص الحساس في البريد الإلكتروني قد مكّن مخترقي أنظمة الكمبيوتر وواضعي برامج الفيروسات أن يطلقوا سلسلة من الأوامر عبر تضمينها في رسالة إلكترونية تستخدم هذه اللغة، ويمكن هنا لبرنامج «ميل اسنشيالز» توفير حماية كاملة لمستخدميه في مثل هذه المواقف، حيث يقوم باكتشاف مثل هذه الأوامر ومحوها بشكل آلي، ومع ذلك يتم إرسال الرسالة للمرسل إليه، ولكن مع تعطيل جميع الأوامر المكتوبة بلغة النص الحساس، وبهذا يتم تأمين الرسالة.

وبفضل هذه الإمكانات الإبداعية الأمنية ينعمُ مستخدمو برنامج «ميل اسنشيالز» بتأمين أجهزة حواسبهم، حتى ضد فيروسات الماكرو كافة وفيروسات لغة النصوص الحساسة التي ستنطلق مستقبلاً، وذلك قبل أن يطرح منتجو برامج محاربة الفيروسات إصدارات تحديث قائمة الفيروسات الخاصة ببرامجهم. وفصلاً عن ذلك يأمن مستخدمو البرنامج شرَّ الهجمات عبر البريد الإلكتروني، وخصوصاً تلك الهجمات الشاملة الموجهة تحديداً ضد الشبكة والتي لا توفر برامج محاربة الكمبيوتر أي دفاع ضدها.

كما يمكن لبرنامج «ميل اسنشيالز» أيضاً أن يقوم باعتراض أية رسائل إلكترونية أو أي من ملحقاتها تستخدم أياً من لغات البرمجة مثل: في. بي V.B (التي استخدمها فيروس الحب) أو لغة لنصوص الخاصة ببرنامج «ويندوز» أو لغة «جافا»، وذلك على مستوى أجهزة تخزين وإرسال الرسائل الإلكترونية الرئيسية (الأجهزة الخادمة) حيث أن هذا البرنامج يعمل كبوابة أمنٍ لفحص محتوى الرسائل قبل وصولها للجهاز الخادم. وهكذا، فإنها تقوم بإنشاء «الجدار الناري» بالنسبة لبرنامج البريد الإلكتروني، حيث تقوم بعزل كل الرسائل المشكوك بها قبل وصولها لمستخدمي البريد الإلكتروني وإصابتهم بأذى.

ويوفر الإصدار الأحدث من هذا البرنامج مزايا إضافية لفحص محتوى الرسائل، مثل القدرة الآلية على محو ملحقات الرسالة الإلكترونية، ويقدم برنامج «ميل اسنشيالز» المزايا التالية:

- تنقية واختبار محتوى الرسائل.
- منع تسرب المعلومات الشخصية.
- فحص جميع الرسائل ضد الفيروسات.
- إجرائيات متقدمة لمنع التعرض للإغراق بالبريد الإلكتروني.
- إخطارات عدم المسؤولية: حيث بإمكانك أن تضيف إخطاراً بعدم المسؤولية مع بريد إلكتروني ترسله.
- إدارة البريد الإلكتروني: التقارير، حفظ وأرشفة جميع الرسائل، إمكانية تحميل بروتوكول 3 للبريد الإلكتروني، ردود آلية عبر الجهاز الخادم.

**2 ـ برامج كمبيوتر توفر الحماية ضد الثغرات الأمنية في البريد الإلكتروني:**

- البرامج التقليدية للحماية ضد الفيروسات التي لا حول لها ولا قوة أمام هذا التهديد الجديد:

أعلنت شركة «جي.إف.آي» J.F.I. والتي تعمل في مجال برامج الكمبيوتر الخاصة، بتأمين البريد الإلكتروني ومحاربة الفيروسات، عن أنها توفر حلاً ضد الجيل الجديد من فيروسات البريد الإلكتروني التي يمكن أن تنتشر حتى لو لم يقم المستخدم بفتح ملحقات الرسالة، حيث يمكن استخدام برنامج شركة J.F.I. لفحص محتوى الرسالة الإلكترونية، والذي أطلقت عليه اسم «ميل اسنشيالز» للحماية ضد هذا التهديد الجديد والخطير على مستوى الجهاز الخادم للبريد الإلكتروني. وقد أوضح رئيس مجلس إدارة الشركة بأنه «وفقاً لتوقعات خبراء أمن الحاسوب، فإن كل جيل جديد من فيروسات البريد الإلكتروني يصبح أخطر وأكثر إيذاءً مما يحتم ضرورة قيام المؤسسات بإحكام إجراءات الأمن الخاصة بالبريد الإلكتروني، وفي الوقت الحاضر فإن نقطة ضعف جديدة يمكن استغلالها لإرسال فيروسات خاصة بالبريد الإلكتروني حتى تبدأ نشاطها.

وكنتيجة لنقطة الضعف هذه، والموجودة في إصدارات شركة مايكروسوفت، فإن أجهزة الكمبيوتر الشخصية التي تستخدم برنامج التصفح «إنترنت إكسبلورر» الإصدار الخام و/أو برنامج «مايكروسوفت أوفيس 2000» عرضة لهجمات الفيروسات التي تستخدم لغة النص الحساس الموجودة ببرامج البريد الإلكتروني حتى لو لم يفتح المتلقي أي ملحقات مع الرسالة التي وصلت.

ومشكلة تأمين البريد الإلكتروني هذه ناجمة عن ثغرة في عملية برمجة معيار التحكم النشط «إكس» الخاص ببرنامج «إنترنت إكسبلورر»، ويسمّى «اسكريبت لت تايب ليب». ولسوء الحظ، ونظراً لسهولة استغلال هذه الثغرة، فإن الوقت سانح لحدث تدميري هائل على الأقل يمكن مقارنته بتأثير فيروس الحب الذي ضرب ضربته في مايو/ أيار 2000.

وليس بوسع البرامج التقليدية للحماية ضد الفيروسات أن تحمي ضد هذه

الأنواع من الفيروسات/ أيار، إلا أن برنامج «ميل اسنشيالز» يمكنه أيضاً أن يقوم باعتراض أية رسائل إلكترونية أو أيٍّ من ملحقاتها تستخدم أياً من ملفات البرمجة مثل V.B. (ڤي. بي) التي استخدمها فيروس الحب، أو لغة النصوص الخاصة ببرنامج «ويندوز»، أو لغة سجافا» وذلك على مستوى أجهزة تخزين وإرسال الرسائل الإلكترونية الرئيسية (الأجهزة الخادمة)، حيث إن هذا البرنامج يعمل كبوابة أمن لفحص محتوى الرسائل قبل وصولها للجهاز الخادم، فإنها تقوم بعمل «الجدار الناري» بالنسبة لبرنامج البريد الإلكتروني، حيث تقوم بعزل كل الرسائل المشكوك فيها قبل وصولها لمستخدمي البريد الإلكتروني وإصابتهم بأذى.

ويُنصح مستخدمو برامج «إنترنت إكسبلورر» و «أوت لوك» بمراجعة الموقع المؤمّن لشركة مايكروسوفت على الإنترنت للحصول على وسيلة مواجهة هذه الثغرة، كما يتعين على مشغلي الشبكات تركيب برنامج يعمل كنقطة تفتيش أمني على محتوى رسائل البريد الإلكتروني، ويكون قادراً على كشف مثل هذا الفيروس للتأكد من عدم انتقال مثل هذه الفيروسات إلى أجهزة تخزين وإرسال البريد الإلكتروني (الأجهزة الخادمة).

**3 ـ شركة J.F.I. (جي. إف. آي) تطلق برنامجها لكشف مخترقي كلمات السر «باس ورد سنيفر» للاستخدام مع برنامج «لانجارد».**

«لانجارد» ليست حائطاً نارياً شخصياً، بل هو برنامج للتحكم في الدخول إلى وكشف متسللي شبكة الإنترنت، وهي مناسبة للاستخدام مع الشبكات، ويتطلب برنامج «لانجارد» نظام تشغيل ويندوز إن تي 2000. ويكشف برنامج «لانجارد» متلصّصي وسارقي كلمات السر على الشبكة ويسمح لإدارة الشبكة باتخاذ ما يلزم من إجراءات ضدهم.

ويشتمل برنامج «لانجارد» للتحكم في الدخول للشبكات والإنترنت حالياً على برنامج لكشف متلصصي كلمات السر، وتمنح هذه الميزة الإضافية

مستخدمي البرنامج تأميناً أفضل لشبكاتهم، حيث إنها تتيح لبرنامج «لانجارد» الكشف عن أي جهاز كمبيوتر على الشبكة مزود ببرامج الكشف عن كلمات السر حيث يمثل مخترقو كلمات السر خطراً أمنياً داهماً، إذ بإمكانهم سرقة كلمات السر الخاصة بشبكة معلوماتك.

ويمكن لمنظمي الشبكة ـ بواسطة لانجارد ـ تحليل المعلومات المنقولة عبر الشبكة والكشف عن بعد أيّ جهاز كمبيوتر على الشبكة في حالة تلصص «أي في حالة تمكنه من رؤية المعلومات المنقولة عبر الشبكة وليس فقط المعلومات المرسلة إليه»، ويتيح لك برنامج لانجارد الاستمرار في مراقبة الشبكة ومسحها لمعرفة الأخطار الأمنية المحتملة.

فعلى سبيل المثال، يتيح البرنامج لمشغّلي الشبكة معرفة أيٍّ من مستخدمي الشبكة يدخلون على مواقع معينة بأجهزة الكمبيوتر. ويعلن رئيس لانجارد عن برنامج لانجارد قائلاً: «تسمح ميزة برنامج لانجارد، بالكشف عن متلصّصي كلمات السر لمديري شبكات الكمبيوتر، الكشفَ عن أولئك الذين يستخدمون برامج الكشف عن كلمات السر على الشبكة، واتخاذ الإجراءات التصحيحية اللازمة؛ «فلانجارد» وهو أداة أمنية لا غنى عنها لضمان أمن شبكات الكمبيوتر، حيث يجب استخدامها بالاشتراك مع حائط ناري، فهناك العديد من برامج اختراق وكشف كلمات السر التي توزع مجاناً على شبكة الإنترنت، لذا لا تستطيع المنظمات والشركات التجارية أن تقف بلا دفاع ضد سرقة كلمات السر.

ويعمل برنامج لانجارد باستخدام تقنية ثورية للتجسس تسمح له بأن يدخل ويستقر داخل أي جهاز كمبيوتر بالشبكة. كما أن البرنامج يتأكد من الاستخدام البناء للانترنت كما يشتمل على ميزات ثورية تستطيع منع البحث عن كلمات وعبارات معينة على الإنترنت. ويشتمل برنامج «فلانجارد» على المميزات التالية:

- يحمي ضد سوء استخدام شبكة الإنترنت.

- يمنع الدخول على مواقع معينة على شبكة الإنترنت.
- يمنع البحث عن، والدخول إلى مواقع معينة ذات محتوى خاص على الإنترنت.
- يمنع إصدار تقارير حول استخدام الإنترنت.
- يوفر تداخلاً أمنياً ممتداً.
- لا يستلزم إعادة توصيف الشبكة.
- لا يؤثر على الأداء.
- لا يستلزم توصيفاً خاصاً من قبل المستخدم.
- يراقب الشبكة ككل.

وعلى أية حال، لم يعد الشخص المتعامل مع الحاسب الآلى بحاجة لبرنامج مكافحة الفيروسات؛ وذلك نظراً لأن معظم شركات إنتاج هذه البرامج، بدأت تحرص على توفير العلاج ضد أى فيروس يكون قد ضرب ضربته الضارة بالفعل، وذلك إما باستخدام برنامج لفحص محتوى رسائل البريد الإلكتروني فيمكن منع وقوع الضرر قبل حدوثه، كما يُمكن لبرنامج الحماية الذي يفحص مضمون الرسائل الإلكترونية، اعتراض أية رسائل أو ملحقاتها تعتمد على لغة برمجةٍ مثل نصوص لغة «فيجوال بيسك» أو أية ملفات أخرى ذات أوامر تنفيذية وذلك على مستوى الجهاز الرئيسي (الخادم).

ومن المؤكد أن الطريقة الوحيدة للحصول على تأمين كامل ضد فيروس الحب، والنسخ المعدلة منه كافة هو اعتراض وإيقاف رسائل البريد الإلكتروني التي تحتوي نصوصاً خاصة بالبرمجة على مستوى الجهاز الرئيسي (الخادم)، وذلك بعزل هذه الرسائل، وهذه هي أكثر الطرق أماناً لمنع الإصابة بهذه الفيروسات.

وبعد هذا الحديث المطوّل عن الفيروسات يُثار تساؤل مهم مؤدّاه: كيف

تمنع المجرمين من الولوج إلى حاسوبك، وكيف تتعرف على أصحاب النيّات الإجرامية على شبكة النت فتأمن شرهم؟

الحقيقة التى يجب أن نشير إليها أن المسألة ليست بالسهولة التي نتصورها، فهذا أمر صعب وهو أحد أسباب خطورة جرائم الإنترنت، حسبما يؤكد المتخصصون؛ ذلك أن المخربين يظهرون بصورة الناصح، أو المرشد مما يتسبب في خداع الضحية، كما أنه لا يمكن التعرف على هوية المخرب، فقد يظهر بهوية مزيفة ويمكن أن يكون التخريب على شكل برامج يتم تحميلها من الإنترنت وتحوي فيروسات، كما يمكن أن تكون على شكل مرفقات مع البريد الإلكتروني.

الواقع أن المخربين على الإنترنت يختلفون من جهة الخطورة؛ فمنهم المستخدم العادي الذي يستطيع الوصول لأغراض تخريبية، ومنهم الهاوي الذي يتعلم بعض المهارات على حساب الآخرين، ومنهم المحترف الذي يقصد التخريب، ومنهم العصابات المنظمة. ولهذا فمن أنجع الوسائل أن يتم التعامل مع الأشخاص على الإنترنت بحذر شديد، وألا يُتعامل إلا مع أشخاص أو مواقع معروفة، بحيث لا يتم تحميل ملفات إلا من المواقع الموثوقة، ويمكن الاستفادة من تقنية التوقيع الرقمي والتي تعطى للمواقع عبر شركات كثيرة، حيث أن المواقع المعروفة لها توقيعات رقمية معترف بها. وهذه التقنية تدعمها برامج تشغيل الحاسبات المنتشرة في العالم، مثل نظام التشغيل ويندوز من شركة مايكروسوفت، ولهذا يتم تحذيرك إذا كان الموقع غير معروف (ليس له توقيع رقمي معروف أو معترف به)، وأيضًا ينبغي التعامل بحذر مع رسائل البريد الإلكتروني بعدم فتح أي بريد يحوي مرفقات حتى لو كان من شخص يعرفه، إلا إذا كان المستخدم يتوقع وصول ذلك البريد، وذلك لاحتمال احتوائها على فيروسات أو ملفات تجسّس.

# الفصل الثالث

# الجرائم الرقمية والإلكترونية في الوطن العربي

يتناول هذا الفصل الجريمة الالكترونية فى الدول العربية عبر ثلاثة مباحث تناول المبحث الأول منها الجريمة الإلكترونية فى مصر، فيما تحدث المبحث الثاني عن تنامي جرائم المعلوماتية والانترنت فى الدول العربية وآليات مواجهتها، وأخيراً ركز المبحث الثالث على إشكالية القصور التشريعى ونمط تعاطي القضاء العربي مع جرائم المعلوماتية.

## المبحث الأول: الجرائم الرقمية والمعلوماتية في مصر وسبل مكافحتها

نتناول في هذا المبحث انتشار جرائم الإنترنت في مصر ثم الآليات التى قررتها مصر لمواجهة الجرائم الالكترونية، وأخيراً موقف القضاء المصري من الجرائم الإلكترونية وضرورات إنشاء محكمة إلكترونية.

### أولاً: انتشار جرائم الإنترنت فى مصر

دخلت خدمة الإنترنت مصر عام 1993 على يد مركز المعلومات ودعم

اتخاذ القرار بالتعاون مع شبكة الجامعات المصرية. ومع بداية عام 1997 بدأ المركز في خصخصة خدمات الإنترنت في مصر، وكانت البداية من خلال 16 شركة زادت إلى 68 شركة في عام 2000، وانتهت إلى 211 شركة هي إجمالي الشركات التي تقدم خدماتها في مجال الإنترنت داخل مصر.

وقد بلغ عدد مستخدمي الإنترنت في مصر في العام الاول لاستخدامه حوالى 75 ألف شخص، ولكنه بعد تطبيق حملة «حاسب لكل بيت» وانخفاض أسعار خدمات الإنترنت السريع، وصل عدد مستخدمي الإنترنت إلي ما يربو على خمسة ملايين و300 ألف مستخدم يحصلون على خدماتهم من خلال 211 شركة تعمل في هذا المجال داخل حدود مصر.

وأكدت مصادر في الإدارة العامة للمعلومات والتوثيق بوزارة الداخلية المصرية، على إن البعض استغلّ ما أتاحه العلم والتقدم التكنولوجي الحديث، استغلالاً سيئًا وبدأ في ارتكاب أعمال أو أفعال ترقى لمستوى الجريمة، وأصبحت تشكل هاجسًا وتحديًا للأجهزة الأمنية. وبات واضحًا أن التهديد القادم شديد الخطورة في ظل ظروف دولية وإقليمية متشابكة، حيث جري الإعداد منذ أكثر من سنتين من أجل تكوين وحدة مباحث جديدة تكون معنية بعملية رصد ومتابعة وضبط كلّ الجرائم المستحدثة بجميع أشكالها وأساليبها والتي يكون الكمبيوتر عنصرًا في ارتكابها، خصوصاً بعد أن بدأت هذه الجرائم تأخذ أشكالاً وأبعادًا دولية وعالمية جديدة وبشكل سريع.

ولعله من نافلة القول الإشارة إلى أهم الجرائم الالكترونية التى انتشرت فى مصر، ومنها جرائم استخدام بطاقات الائتمان المملوكة للغير، حيث يتم سرقتها واستخدامها في شراء سلع وخدمات من الخارج، ثم ظهرت بعض الجرائم الأخرى ذات الصلة بالكمبيوتر، مثل جرائم الشبكات واختراقها والدخول على أجهزة الحاسب الآلي للغير وسرقة المعلومات التي تمثل سرية خاصة لبعض الأشخاص أو المؤسسات أو الشركات، كما ظهرت جرائم

الإنترنت وقيام البعض بنشر مواقع تسيء لأشخاص آخرين أو تسيء لشكل ومظهر الدولة، ثم ظهرت جرائم عالمية أخرى يقوم بها بعض الهاكرز ومنها إطلاق الفيروسات والاختراقات، ومنها اختراق المواقع الرسمية أو الشخصية أو اختراق الأجهزة الشخصية وأنظمة شفرات الكمبيوتر للمؤسسات والأفراد، وجرائم التجسس الصناعي، وجرائم الأموال، مثل السطو والاحتيال والنصب وسرقة بطاقات الائتمان والتزوير والجريمة المنظمة، وجرائم المخدرات وغسل الأموال، وجرائم الآداب وتجارة السلاح وجرائم الابتزاز الإلكتروني، وجرائم الغش الإلكتروني، بالإضافة إلى جرائم القرصنة وجرائم محتوى الإنترنت من المواقع الإباحية أو المعادية سواء دينيًا أو سياسيًا.

ويجب التأكيد على أن إدارة المعلومات والتوثيق بوزارة الداخلية تحتضن مجموعات عمل تعكف على متابعة شبكة الإنترنت على مدار اليوم لمراقبتها وفحص التعاملات والمعاملات التي تتم عليها، مِنْ وإلى الخارج، وإذا ما ظهرت أية مخالفات أو أعمال تمثل خروجًا على القانون والشرعية أو تهديد أمن واستقرار الوطن يتم التدخل فورًا بالتنسيق مع الأجهزة النوعية الأخرى.

ومما لا شك فيه أن التأثير المجتمعي الذي يحدثه التقدم التكنولوجي يحتاج إلي تنظيم قانوني، يضع إطاراً للعلاقات التي تترتب علي استخدامه بما يكفل حماية الحقوق المترتبة على هذا الاستعمال، ويحدد الواجبات تجاهها، فلا بدّ للتقدم العلمي والتكنولوجي أن يواكبه تكيف في القواعد القانونية، إذ لا يجوز للقانون أن يقف صامتاً مكتوف الأيدي حيال أساليب انتشار هذا التقدم، وحيال القيم التي يروجها.

ولا يقتصر دور القانون على مجرد تنظيم العلاقات المترتبة علي التقدم التكنولوجي بل يتوجب أن يحمي القيم التي تحيط باستخدام التكنولوجيا، ويحدد المسار الصحيح الذي يجب أن يسلكه التقدم التكنولوجي حتى لا يتخذه المجرمون أداة لتطوير وسائل إجرامهم، بل يكون على العكس من ذلك، وسيلة

لمحاربة هذا الإجرام، وهو ما يوجب على القانون أن تمتد نصوصه إلى الأنشطة الجديدة التي تفرزها التكنولوجيا حتي تحدد الجريمة في نصوص منضبطة واضحة، ولا يُترك بحثها إلى نصوص قانون العقوبات التقليدي، التي قد تتسم بعدم اليقين القانوني أو لا تتسع لملاحقة الأنماط الجديدة من الإجرام.

وعلى أية حال، استطاعت الشبكات الإلكترونية أن تغير من دور الدولة كأمة ومن سيادتها، لأنها أدت إلي انتشار فاعلين جدد عابرين للأوطان وإلى إنشاء نماذج دولية جديدة مثل مجتمع الإنترنت. وقد تتجاوز نتائج هذه الجرائم إلي وقوع جرائم أخرى تهدد الحق في الحياة والسلامة البدنية، إذا ما أدى العبث في المعلومات إلى تغيير طريقة العلاج أو تركيبة الدواء.

وحذر خبراء مصريون من أن جرائم الإنترنت قد تؤثر علي نطاق الخدمات الإلكترونية وقطاعات التنمية الاقتصادية، وتكنولوجيا المعلومات، بخاصة أن مصر تطرح نفسها الآن كمركز متميز في مجال التكنولوجيا، الأمر الذي يتطلب إعادة هيكلة قطاع الاتصال، وتدعيم دور الدولة في حماية مستخدمي تكنولوجيا الاتصالات، من خلال إجراءات تتميز بالشفافية الكاملة، خصوصاً أننا نواجه تحديات جديدة بما يُعرف بالجريمة الإلكترونية، التي يجب مكافحتها، لتشجيع الاستثمار وحماية حقوق الملكية الفكرية، الأمر الذي يستلزم ألا يتم بمعزل عن الثوابت التشريعية والقانونية.

ومما يذكر، أن التقدم التكنولوجي، قد أفرز أنماطاً جديدة من الجريمة، وكذا من المجرمين، فكان للتقدم في مختلف العلوم أثره علي نوعية الجرائم، ومن ثم فقد استغلّ المجرم المعلوماتي ثمرات هذه العلوم في تطويع المخترعات العلمية الحديثة لخدمة أهدافه الإجرامية، فالمشكلة الرئيسية لا تكمن في استغلال المجرمين الإنترنت، وإنما في عجز أجهزة العدالة عن ملاحقتهم، وعدم ملاحقة القانون إياهم ومواكبة التكنولوجيا الجديدة لتشريعاته. فالقانون الجنائي لا يتطور دائماً بالسرعة نفسها التي تتطور بها التكنولوجيا الحديثة،

لاسيما أن نصوص القانون الجنائي التقليدي وضعت في عصر لم يكن الإنترنت فيه قد ظهر إلى الوجود، كما لم تظهر بعدُ المشاكل القانونية الناشئة عن استخدامه، مما يفرض على رجال القانون التدخل لمكافحة الجرائم الناشئة عن استخدام الإنترنت ومواجهة هذا النقص التشريعي، خصوصاً أنه لا يوجد لدينا نصوص خاصة بهذه الجرائم.

ومن ثَمّ، فقد تعولمت الجريمة وظهرت أنماط جديدة منها، وأصبحت الجريمة تنفذ عن بُعْدٍ من دون الحاجة إلى الفعل الفيزيقي بموضوع الجريمة، مثل غسيل الأموال وتحويلها عبر الإنترنت، وسرقة البنوك والحسابات التي لم تعد تتطلب السطو على البنك في موقعه الفعلي، وإنما يمكن أن يكون ذلك إلكترونياً بتحويل أرصدة من الحسابات إلي حسابات أخرى في دول أخرى. فضلاً عن ذلك فقد ظهرت جرائم التعدي على الحاسب والجرائم المرتبطة به، وجرائم الملكية الفكرية وجرائم قرصنة الحاسب والتجسس العسكري والإلكتروني. . هذه الأنماط شكلت كلّها تحدياً جديداً في تفسير الجريمة، وفي وسائل الوقاية والمكافحة، لكننا نرى أن البعض يتعامل مع هذا الخطر بسلبية وبطء شديدين، لا يتماشيان مع خطورة وأهمية المرحلة؛ فهناك قصور واضح عربياً في مجال جرائم الإنترنت سواء من حيث أساليب التحقيق والرصد أو في مجال التوعية والتثقيف، وظهرت الحاجة إلى تثقيف القائمين بالضبط، والخبراء وسلطات التحقيق، على التعامل وتفهّم هذا النوع من المشاكل التي تحتاج إلى خبرات فنية عالية حتى تتكون لديهم درجة من المعرفة الفنية تتناسب مع حجم المتغيرات والتطورات المتلاحقة في مجال جرائم تقنية المعلومات والإنترنت.

وهنا تبرز أهمية نشر الوعي المجتمعي بالمخاطر الاقتصادية والاجتماعية والثقافية وغيرها، الناجمة عن الاستخدامات غير الآمنة للإنترنت، وتكثيف التوعية عن الآثار السلبية الناتجة عن تلك الجرائم، لذلك تضافرت الجهود في مصر لكي يكون هناك دور أهليّ تطوعيّ للقيام ضد مظاهر العدوان الإجرامي

عبر الإنترنت عن طريق إنشاء الجمعيات والمراكز المهتمة بمكافحة الجرائم عبر الإنترنت.

## ثانياً: التكييف القانوني للجرائم الإلكترونية فى مصر وآليات مواجهتها

على الرغم من هذا الكمِّ الرهيب من الجرائم التي ترتكب على شبكة الإنترنت إلا أن هناك فراغاً تشريعياً في مواجهة هذه الجرائم التي مازالت تخضع لقانون العقوبات العادي الذي بات غير قادر على مواجهة هذه النوعية من الجرائم المستحدثة التي تحتاج فى تكييفها إلى قانون محدد.

وعلى الرغم من انتشار هذه الجرائم في مصر فى ظل جهود الحكومة المصرية من أجل جذب الاستثمارات في مجال التكنولوجيا، إلا أن هناك فراغاً تشريعياً في هذا المجال، خصوصاً في قضايا النشر الإلكتروني وقوانين جرائم الإنترنت الخاصة باقتحام النظم وغيرها. فالحقيقة أن مصر لا يوجد فيها نظام قانوني خاص بجرائم المعلومات، إلا أن القانون المصري يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعا من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكوِّنة لأركان الجريمة المعلوماتية.

وقد أرجع المتخصّصون هذا الفراغ من أية عقوبات خاصة بجرائم الإنترنت فى التشريع المصري، إلى حداثة هذا المجال الذي لا يكاد يتعدّى عمره سنوات قليلة، وما يطبق حالياً على جرائم الإنترنت هو القانون التقليدي الذي يتم بموجبه الحكم على الجرائم العادية، مثل جريمة سرقة، حيث يعاقب مرتكبها بالحبس مدة لا تقل عن 24 ساعة ولا تزيد على ثلاث سنوات وجريمة النصب التي يعاقَبُ مرتكبها بعقوبة النَّصْب المدرجة في قانون العقوبات.

أما السبُّ والقذف الإلكتروني، فتعتبر جنحةً، وإذا كانت الجريمة تركيب صور فاضحة، توجّه لمرتكبها تهم خدش الحياء وهتك العرض والتحريض على

الفسق. أما إطلاق الشائعات والسطو على أرقام البطاقات الائتمانية واقتحام نظم البنوك، فتوجه إلى مرتكبها تهم تكدير الأمن العام وتهديد الاقتصاد القومي والإضرار بالمصالح العليا للبلاد، وهي اتهامات خطيرة تقود صاحبها إلى محاكم الجنايات مباشرة. على أن هذا التكييف القانوني لجرائم المعلوماتية يظل عاجزاً عن مواكبة هذه النوعية من الجرائم وما يصاحبها من تطور مستمر، فضلاً عن تنامي أنواعها وانتشارها بشكل مريب، وهو الأمر الذي يحتم على المُشرِّع المصري سرعة إصدار قانون جديد يواجه الجرائم الإلكترونية، خصوصاً أن هناك بعض الجرائم المستحدثة التي لن تجد لها تكييفاً قانونياً محدداً في القانون التقليدى.

**آليات مكافحة الجريمة الإلكترونية فى مصر:**

فيما يتعلق بآليات مواجهة الجرائم المعلوماتية، فلا أحد ينكر الجهود الحكومية والأهلية فى مجال المكافحة. فقد أنشأت وزارة الداخلية المصرية عام 2002، آليّة فى هذا الإطار تحت مسمى «إدارة مكافحة جرائم الحاسب الآلي وشبكة المعلومات التابعة للإدارة العامة للمعلومات والتوثيق، بالقرار الوزاري رقم 13507 لسنة 2002[1].

وقد تحددت مهام الإدارة فى رصد ومتابعة جرائم التطور التكنولوجي وتتبع مرتكبيها من خلال أحدث النظم الفنية والتقنية الحديثة، ويتم تقنين الإجراءات بعد عملية التتبع الفني وضبط القائم بارتكاب الجريمة التي يكون تكييفها القانوني من خلال قانون العقوبات والجريمة، التي تتعامل معها الإدارة تتمثل فى الأنشطة غير القانونية التي يكون فيها الكمبيوتر وسيلةً أو غايةً أو كليهما معاً، وتتخذ أشكالاً متعددة، بما فيها الاحتيال باستخدام البطاقات الائتمانية وبيع المواد الإلكترونية، وانتهاك حقوق الملكية الفكرية في مصر، وسرقة البريد

---

(1) راجع: قرار وزير الداخلية المصري الرقم 13507 لسنة 2002 بشأن إدارة مكافحة جرائم الحاسب الآلي وشبكة المعلومات التابعة للإدارة العامة للمعلومات والتوثيق، القاهرة 2002.

الالكتروني والتزوير باستخدام الماسحات الضوئية والطابعات وجرائم الشبكات واختراقها والدخول على أجهزة الحاسب الآلي للغير، وسرقة المعلومات التي تمثل سرية خاصة لبعض الأشخاص أو المؤسسات أو الشركات، وقيام البعض بنشر مواقع تسيء لأشخاص آخرين أو تسيء لشكل ومظهر الدولة. ثم ظهرت جرائم عالمية أخرى يقوم بها بعض الهاكرز، ومنها إطلاق الفيروسات واختراق المواقع الرسمية أو الشخصية أو اختراق الأجهزة الشخصية وأنظمة شفرات الكمبيوتر للمؤسسات والأفراد، وجرائم التجسس الصناعي، وجرائم الأموال، مثل السطو والاحتيال والنصب والجريمة المنظمة، وجرائم المخدرات وغسيل الأموال، وجرائم الآداب وتجارة السلاح وجرائم الابتزاز الإلكتروني، وجرائم الغش الإلكتروني، بالإضافة إلى جرائم القرصنة وجرائم محتوى الإنترنت من المواقع الإباحية أو المعادية، سواءٌ دينيًا أو سياسيًا.

## آلية عمل الإدارة ومراحل التحري والضبط

تمر القضايا التي ترد إلى إدارة مكافحة جرائم الحاسب الآلي وشبكة المعلومات، بالعديد من الإجراءات، منها: فحص البلاغ في القسم الفني، وتأكيد المعلومات الواردة به، ثم تثبيت الاتهامات عبر القسم الجنائي، ومهمته تحرير المحضر، ثم يعود الملف على القسم الفني مرة أخري لمتابعة الإيميلات ونصب الكمائن الإلكترونية، وتحديد شخصية المتهم، وعنوانه، واعداد تقرير فني برقم التليفون المستخدم في الدخول على الإنترنت، أو مكان مقهى الإنترنت المستخدم في ارتكاب الواقعة. ومن ثمّ يقوم القسم الجنائي بالتعاون مع قسم العمليات، حيث يتم استصدار إذن من النيابة العامة بضبط جهاز الحاسب الآلي المستخدم في ارتكاب الجريمة، وفحصه، وبعد ذلك يتم تسليم الجهاز إلى القسم الفني ليتولّى مثل هذه العمليات، واستخراج الأدلة والصور التي تدين المتهم، ثم يتم إعداد تقرير فني استكمالي لإرفاقه مع المتهم الذي يتم إحالته للنيابة للتحقيق.

فضلاً عما تقدم، يتم ضبط الجريمة من خلال بلاغ أو معلومة تصل إلى جهاز الأمن، وتقوم الإدارة بتتبعها وإثباتها بالأدلة وبالأسلوب التقني والفني ومدي الجرم والمخالفة التي تمت وتقديم مرتكبها إلى المحاكمة. ومما يساعد على السرعة فى الإنجاز والأداء أن الإدارة تضم نخبة متميزة من الضباط والفنيين المدربين علي مكافحة جرائم الانترنت، وكيفية التعامل مع أحدث اجهزة الفحص الفني الموجودة في الوزارة للتعامل مع مثل هذه الجرائم والتحفظ عليها بشكل آمن، وسحب كل البيانات، والمعلومات، والصور، بطريقة سليمة لضمها إلي ملف القضية.

**بعض النماذج لجرائم إلكترونية فى مصر وآلية التعامل معها:**

1 ـ حررّت ربّة منزل محضراً رسمياً في إدارة مكافحة جرائم الحاسبات وشبكات المعلومات في الإدارة العامة للمعلومات والتوثيق بوزارة الداخلية، أكدت فيه تضررها من قيام زوجها السابق بالتشهير بها عن طريق الإنترنت، وقد تبين من الفحص الفني وجود ثلاثة مواقع إباحية بشبكة الإنترنت تحتوي على أفلام مُخلِّة لها وتعليقات على تلك الأفلام تتضمن عبارات تشهير بها وبزوجها الحالي، كما تبين أن المتهم، وهو زوجها السابق ويعمل تاجر أدوات منزلية، ارتكب الواقعة انتقاماً من الشاكية لوجود بعض القضايا والخلافات بينهما، فضلاً عن قيامها بالزواج من آخر.

2 ـ لجأت فتاة حاصلة على بكالوريوس تجارة إلى الإدارة نفسها لتحرر محضراً بتضررها من قيام مجهول بإنشاء بروفيل لها على موقع «الفيس بوك» من خلال شبكة الإنترنت، متضمناً بياناتها الشخصية وصوراً شخصية خاصة بوالديها وعبارات توحي برغبتها في إقامة علاقات محرّمة مع من يرغب. وقد أثبت الفحص الفني أن مرتكب الواقعة، وهو خطيب الشاكية السابق، قد استخدم جهاز حاسب آليٍّ متّصل بشبكة (ADSL) فيها خمسة

عشر مشتركاً. وقد اعترف بارتكابه الواقعة، مبّرراً ذلك بالانتقام من الشاكية وأسرتها لرفضهم تسليمه «الشّبْكة» عقب قيامه بإنهاء الخطبة.

3 ـ مواطنة حاصلة على بكالوريوس هندسة تتضرر من قيام مجهول بإرسال رسائل بريد إلكتروني على عنوان البريد الإلكتروني الخاص بها تتضمن عبارات سب وقذف، فضلاً عن تهديدها ببعض الصور الشخصية لها.

والجدير بالملاحظة أن إدارة مكافحة جرائم الحاسب بوزارة الداخلية، تستطيع الوصول إلى الشخص الذي يرتكب جريمة إلكترونية عن طريق الـ(I.P) وهو العنوان الإلكتروني لهذا الشخص؛ فبمجرد دخول أيّما شخص على الإنترنت يحصل على رقم خاص به وعن طريق هذا الرقم يتم تحديد موقعه.

وتشير مصادر بوزارة الداخلية إلى أن جرائم انتهاك حقوق الملكية الفكرية خصوصاً قرصنة البرمجيات، أدت إلى خسائر كبيرة في منطقة الشرق الأوسط وأفريقيا، وهاتان المنطقتان تعدان من المناطق التي شهدت ارتفاعاً كبيراً في معدل قرصنة المعلومات بين عامي 2005 و2006، حيث وصلت نسبة انتشار البرمجيات المقلَّدة إلى 60 ٪ في منطقة الشرق الأوسط.

ومن مظاهر الجهود المبذولة من الإدارة الجديدة، تشكيل مجموعات عمل لمتابعة شبكة الإنترنت يوميًا على مدى اليوم. لمراقبتها وفحص التعاملات والمعاملات التي تتم عليها مِنْ وإلى الخارج، وإذا ما ظهرت أية مخالفات أو أعمال تمثل خروجًا على القانون والشرعية أو تهديد أمن واستقرار الوطن، يتم التدخل فورًا بالتنسيق مع الأجهزة النوعية الأخرى[1].

ويأتي فى إطار الآليات الخاصة بمواجهة الجرائم الإلكترونية فى مصر، آلية الابلاغ عن الجرائم، حيث بإمكان المواطنين الإبلاغ عن الجرائم الإلكترونية عبر الوسائل الآتية:

(1) http://www.ahlalhdeeth.com/vb/showthread.php?t = 169760.

1 ـ الموقع الإلكتروني لوزارة الداخلية على شبكة الإنترنت (WWW.Moiegypt.gov.eg).

2 ـ إخطار إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بمقر وزارة الداخلية بشارع الشيخ ريحان، سواء بالحضور الشخصي أو الاتصال بأرقام تليفونات: 27928484/ 27926071/ 27924090/ 27924091.

3 ـ كما يمكن تلقي البلاغات من خلال الخط الساخن (108) والذى تم إنشاؤه مؤخرا لهذا الغرض.

**ولا يمكن إنكار الدور الذى تمارسه الجمعية المصرية لمكافحة جرائم الإنترنت فى مجال التصدى لهذا النوع من الجرائم، باعتبارها إحدى الآليات الأهلية التي بذلت جهوداً فنية وبحثية من أجل الحد من جرائم المعلوماتية والإنترنت، ويمكن رصد بعضٍ من هذه الجهود فى النقاط التالية:**

1 ـ وقعت الجمعية بروتوكول تعاون مع كلية الحقوق، جامعة عين شمس، بهدف تثقيف وتدريب طلبة وخريجي كليات الحقوق و الآداب والإعلام والسياحة والآثار والتجارة والحاسبات والمتخصصين، والسادة القضاة وأعضاء النيابة العامة والسادة المحامين والعاملين في القطاعات القانونية في المؤسسات، وتأهيل وإكساب المتدربين المهارات القانونية والعلمية والعملية والفنية الخاصة بارتباط المعلوماتية والاتصالات بتخصصاتهم، ومدى تأثير استخدام تكنولوجيا المعلومات في إنجاز مهام أعمالهم والتعريف بماهية التعامل مع الإشكاليات القانونية في حقل المعاملات الإلكترونية حول موضوعات تشمل كيفية إثبات الشخصية، كيفية التوقيع الإلكتروني، أنظمة الدفع النقدي الرقمي(المال الرقمي أو الإلكتروني)، سِرّيةِ وأمن المعلومات من مخاطر إجرام التقنية العالية، خصوصية العميل، المسؤولية عن الأخطاء والمخاطر، حجية المراسلات الإلكترونية، التعاقدات المصرفية الإلكترونية، مسائل الملكية الفكرية

لبرمجيات وقواعد معلومات البنك أو المستخدمة من موقع البنك أو المرتبطة بها، علاقات وتعاقدات البنك مع الجهات المزودة للتقنية أو المورّدة لخدماتها أو مع المواقع الحليفة، مشاريع الاندماج والمشاركة والتعاون المعلوماتية.

2 ـ مبادرة انطلقت من القاهرة كمبادرة دولية تبنتها الجمعية الدولية لمكافحة الإجرام السيبيرى بفرنسا، بالتعاون مع الجمعية المصرية لمكافحة جرائم الإنترنت، تحمل بارقة أمل لِسنّ قوانين رادعة تحمى رواد شبكة الإنترنت من التجاوزات غير اللائقة التي تحدث على الشبكة، بداية من الإرهاب الإلكتروني ومروراً بالسطو على الحقوق الفكرية، وانتهاءً بتجريم تجارة الرقيق الأبيض على الشبكة العنكبوتية، وماهية التنظيم القانوني للعالم الافتراضي بأقسامه؛ من المعاملات القانونية الرقمية وعقود التجارة الإلكترونية وحماية الملكية الفكرية عبر الإنترنت، والتعريف بأنماط وأشكال الجرائم عبر الإنترنت وماهية الدليل الرقمي وحجيته في الإثبات، وعرض أحدث التقنيات الفنية العالمية للتعامل مع مثل هذه النظم.

وغنيٌّ عن البيان أن الكثير من أهل الاختصاص فى مجال جرائم المعلوماتية والإنترنت، قد اقترحوا آلية متخصصة تماماً فى هذا المجال هى «شرطة الإنترنت» كجهة مسؤولة عن مكافحة جرائم الإنترنت.

## ثالثاً: القضاء المصري والجرائم الإلكترونية: نحو ضرورة إنشاء محكمة إلكترونية

بدايةً، يجب التأكيد على أن إدارة مكافحة جرائم الحاسبات وشبكات المعلومات في الإدارة العامة للمعلومات والتوثيق بوزارة الداخلية، تعمل على تطبيق القوانين الحالية، ومنها قانون العقوبات رقم 58 لسنة 1937، وقانون حماية حقوق الملكية الفكرية رقم 82 لسنة 2002، وقانون تنظيم الاتصالات رقم 10

لسنة 2003، وقانون تنظيم التوقيع الإلكتروني رقم 15 لسنة 2004، والقانون رقم 126 لسنة 2008 بتعديل قانون الطفل رقم 12 لسنة 1996، فضلاً عن قوانين أخرى ـ من المقرر الانتهاء منها ـ وتشمل قانون الجريمة الإلكترونية وإجراءاتها الجنائية، وقانون التجارة الإلكترونية، وقانون حماية البيانات الشخصية، وتأمين الفضاء الإلكتروني، ويتم اعداد وصياغة تلك القوانين من خلال تعاون وثيق بين أجهزة الدولة التشريعية والتنفيذية والفنية. ومن المؤكد أنه باكتمال صدور تلك التشريعات تكتمل منظومة مكافحة الجرائم الإلكترونية فى مصر.

ومن الجدير بالذكر أن ساحات القضاء المصرى شهدت عشرات القضايا الناجمة عن جرائم الكترونية أغلبها قضايا متعلقة بالتشهير بالأفراد أو النصب والاحتيال؛ فمثلاً شهد عام 2005، صدور أول حكم لجرائم التشهير عبر الإنترنت عندما قضت محكمة جُنح مستأنف النزهة بمعاقبة الفلسطيني فيصل عدنان بالحبس لمدة ستة أشهر لإدانته بنشر صور إباحية ومعلومات خاصة عن فتاة خليجية على شبكة الإنترنت. وقد بدأت القضية ببلاغ من الفتاة لمباحث المصنفات الفنية.

وتأتي ضمن القضايا التي لاقت اهتماماً إعلامياً، قضية اقتحام الموقع الإلكتروني لمجلة روز اليوسف التي حدثت في نهاية عام 2005، فقد تقدمت المؤسسة ببلاغ لإدارة مكافحة جرائم الحاسبات وشبكة المعلومات عن قيام مجهول باختراق موقع المجلة وتغيير المواد المنشورة، وتمكن ضباط المباحث من خلال التحليل والفحص الفني من تحديد الأرقام التعريفية التي استخدمت في عملية الاختراق وتم ضبط المتهم والجهاز المستخدم بمقر الشركة التي يعمل بها وبفحص الجهاز أمكن التوصل لادلة إثبات أنه هو الشخص الذي اخترق موقع مجلة روز اليوسف[1].

(1) http://www.ng3awya.com/topic29076.html.

**ويؤكد الكثير من رجال القانون على ضرورة إنشاء محكمة إلكترونية لسدّ الفجوة القانونية التي أحدثها التطور التكنولوجي الهائل في السنوات الأخيرة،** فهناك جرائم تُرتكب، وحرمات تُنتهك، وحقوق تُسلب على شبكة الإنترنت دونما رقابة قانونية تذكر، والسبب في ذلك عدم وجود قانون دولي رادع يلاحق هواة الإجرام الإلكتروني، ويحاكمهم أمام محاكم دولية، إلا أن ذلك ليس من الأمور البعيدة التي يمكن أن تشق طريقها إلى التطبيق العملي في المستقبل القريب[1].

والمحكمة الإلكترونية التي نتحدث عنها، تتطلب ـ بشكل عاجل ـ إصدار تشريعات متخصصة فى مجال مكافحة الجريمة الإلكترونية، فضلاً عن توفير القضاة المتميزين للقيام بأعمال الفصل فى القضايا المطروحة على هذه المحاكم، على أن يتم تنظيم الدورات اللازمة لتأهيل القاضي الإلكتروني وتمكينه من ملاحقة التقدم الكبير فى مجال الجرائم الإلكترونية.

إن الانتشار الكبير للإنترنت في الحياة العملية، أظهر الحاجة إلى وضع الحلول القانونية للمشاكل الناتجة عن استخدام الإنترنت في ضوء القواعد العامة للقانون فضلاً عن أهمية توجيه نظر المشرّع للتدخل لوضع قواعد خاصة لتنظيم استخدام الإنترنت في بعض المجالات الحيوية، كما أن عليه وضع بعض النقاط صوب عينيه في تشريع قانون حماية المعلومات، وهي الحماية المدنية لمواقع الإنترنت والإثبات والضوابط الشرعية لاستخدام الإنترنت والتقنية والجريمة المنظمة وتفعيل قانون العقوبات.

وإذا كانت هناك جرائم ذات طابع اقتصادي أو سياسي تلقى اهتمامًا واسعًا من المؤسسات المعنية بمكافحة جرائم الإنترنت، فإن الجرائم الأخلاقية على الإنترنت والتي يقوم بها أكبر مسوّقي تجارة الجنس في العالم، كثيرًا ما تصطدم

---

(1) http://www.moheet.com/show_news.aspx?nid=111727&pg=38

بعوائق تشريعية. ففي مصر مثلاً، قامت شرطة الآداب بمراقبة عشرة آلاف شاذ من المتغربين يعلنون عن عناوينهم على الإنترنت ويبدون استعدادهم لممارسة الفجور، لكن الشرطة لم تستطع إحالتهم إلى المحاكم لأنها لم تستطع إصدار إذن من النيابة لمعاقبتهم؛ لأنهم يمارسون فعلتهم الشنعاء من مواقع خاصة. أما تنظيم الشواذ الذي ألقي عليه القبض بالفعل فقد تجاوزوا الدعوة والتعارف على الإنترنت إلى الالتقاء الفعلي وهو ما مكّن الشرطة من إحالتهم إلى القضاء.

## المبحث الثانـي:
## تصاعد معدلات الجرائم الرقمية والمعلوماتية في الوطن العربي ووسائل مكافحتها

ليست الدول العربية ببعيدةٍ عن مرمى الجرائم الإلكترونية، ذلك أن هذه الجرائم لم تترك بلداً من بلاد العالم إلا واخترقتها ونالت من أهداف محددة فيها؛ فالسعودية والإمارات وسلطنة عمان والكويت وفلسطين وغيرها من الدول العربية بادرت إلى وضع ـ أو في طريقها لوضع ـ تشريعات إلكترونية لمواجهة الجرائم المعلوماتية.

وبالنظر إلى موقع العالم العربي في خريطة استخدام وسائل تقنية المعلومات الحديثة، وموقع الدولة بين شقيقاتها الدول العربية، فإن إحصائيات الاتحاد الدولي للاتصالات لعام 2001 تشير إلى أن نسبة مواطني العالم العربي، الذين سبق أن استخدموا شبكة الإنترنت، لا يتعدى 1٪ رغم أن سكان العالم العربي ال 170 مليون نسمة يشكلون 5٪من مجموع سكان العالم.

وإذا ما قارنا ذلك بنسبة الأوروبيين والأمريكيين التي تفوق 58 في المائة فإن ذلك يدفع البعض إلى وصف تجربة العالم العربي في مجال تكنولوجيا الاتصالات والإنترنت بأنها في مرحلتها «الجنينية».

وإذا لم يكن الحاجز أخلاقياً أو سياسياً فقد يكون تقنياً أو مالياً. إذ تُعدُ معظم شبكات الاتصال في العالم العربي غير متطورة وملكاً للقطاع العام. كما تتباين نسبة توفير خدمات الاتصال من بلد عربي لآخر؛ ففي الوقت الذي نجد فيه أكثر من 100 خط هاتفي لكل 100 منزل في الإمارات والكويت، لا تتعدى النسبة في سوريا ومصر والمغرب حيث الكثافة السكانية كبيرة، خمسين خطاً هاتفياً لكل مائة عائلة.

كما أن نفقات الاتصال لا تزال عالية في بلدان العالم العربي، ما يحول دون التشجيع على استخدام الإنترنت بشكل مكثف. فقد تبلغت كلفة ثلاثين ساعة اتصال بالإنترنت شهرياً في سوريا 47 دولارا أمريكيا، وفي السعودية 41 دولاراً، و 24 دولاراً في الإمارات العربية المتحدة، وعشر دولارات في مصر.

ووفقاً لدراسةٍ، أُعدت لصالح منتدى دافوس الاقتصادي الدولي حول تحديات تطور تكنولوجيا الاتصالات والإعلام في العالم العربي، تم تصنيف الدول العربية إلى مجموعات ثلاث: مجموعة التطور السريع وتشمل الكويت والإمارات العربية المتحدة، ومجموعة الدول الصاعدة، وتشمل كلاً من مصروالأردن ولبنان والسعودية، ومجموعة الدول السائرة في طريق النمو وتضم المغرب وعمان وسوريا.

ويمكننا بيان تطور الجرائم الإلكترونية فى الدول العربية ووسائل تعاطيها معها من خلال النقاط التالية:

## أولاً: المملكة العربية السعودية

أعلنت السلطات المختصة أنها ستفرض عقوبات بالحبس لمدة عام واحد وغرامات لا تزيد عن 500 ألف ريال، فيما يعادل 133 ألف دولار، لجرائم القرصنة المرتبطة بالإنترنت وإساءة استخدام كاميرات الهواتف المحمولة مثل التقاط صور دون تصريح، إلا أن المملكة وفى رغبة من أجل تقنين هذا الوضع،

أصدرت تشريعاً وطنياً فى هذا الخصوص، في الآونة الأخيرة، تحت مسمى «نظام مكافحة جرائم المعلوماتية السعودي».

وبإصدار هذا التشريع تكون المملكة العربية السعودية[1]، قد سبقت نظيراتها من الدول العربية فى إصدار قانون جديد لمكافحة جرائم المعلوماتية التي تشمل التهديد والابتزاز والتشهير بالآخرين في مواقع الإنترنت وإنشاء مواقع الإنترنت الإرهابية.

وذكرت مصادر في وزارة الداخلية السعودية أن نظام مكافحة جرائم المعلوماتية قد أصبح قيد التطبيق بعد صدور موافقة مجلس الوزراء عليه، باعتباره إطاراً قانونياً مهماً جداً في تعريف وتحديد الجرائم المعلوماتية والحدّ منها ومواجهتها بعد أن أصبحت تلك الجرائم من بين الجرائم التي تهدد أمن وسلامة المجتمعات الإنسانية.

ويشمل النظام الجديد 16 مادة تتضمن عقوبات صارمة ضد مرتكبي هذه الجرائم تتراوح بين سنة و10 سنوات سجناً، وغراماتٍ مالية تصل الى خمسة ملايين ريال سعودي، مضيفاً أن النظام تضمن تعريفات المصطلحات والمسميات الواردة في النظام مثل «الشخص» و«النظام المعلوماتي» و«الشبكة المعلوماتية» و«البيانات والجريمة المعلوماتية، إلى جانب أهداف النظام بالحدّ من هذه الجرائم والعقوبات المقررة لكل منها.

وحدّدت مواد النظام الأخرى الجرائم المعلوماتية وعقوباتها التي تنوعت بين السجن لمدد مختلفة والغرامات المالية بحسب نوع وطبيعة كل جريمة من الجرائم المعلوماتية واختصاصات كل من «هيئة الاتصالات وتقنية المعلومات»

---

(1) راجع: «نظام مكافحة جرائم المعلوماتية السعودي» الصادر بالمرسوم رقم م/ 17 بتاريخ 8/ 3/ 1428هـ وطبقاً لقرار مجلس الوزراء رقم (79) بتاريخ 7/ 3/ 1428هـ، قائمة الملاحق.

و«هيئة التحقيق والادعاء العام» في المساندة اللازمة للأجهزة الأمنية لتحقيق أهداف وغايات هذا النظام.

ويهدف النظام الجديد إلى حماية المجتمع من جرائم المعلوماتية والحدّ منها والمساعدة على تحقيق الأمن المعلوماتي وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية، وحماية المصلحة العامة والأخلاق والآداب العامة وحماية الاقتصاد الوطني.

ولقد عانت السعودية فى الفترة الأخيرة من محاولات اختراق مواقع الإنترنت، وكان آخرها، عندما تعرض أحد المواقع التعليمية الحكومية بالسعودية لاختراق استمر عدة ساعات كتب خلالها من قام بالاختراق ورمز لنفسه بالرمز (0) عبارات ينصح من خلالها المشرفين على الموقع الاهتمام بالموقع وحمايته وعدم استخدام برامج تصميم مجانية. وتأخر كثيراً مشرفو موقع إدارة التربية والتعليم بمنطقة تبوك، وهو الموقع الذي تم اختراقه، في صيانة الموقع وحل مشكلة الاختراق، حيث ظل فترة طويلة ورسالة الاختراق ظاهرة على واجهته.

الجدير بالذكر أن مواقع حكومية كثيرة قد تعرضت أخيراً للاختراق، إما بداعي التطفل أو لوجود كثير من الخلافات بين الجهة الحكومية ومن يقف خلف هذا الاختراق، خصوصاً في المواقع التعلمية الحكومية، ما اضطرّ مسؤولي وزارة التربية والتعليم السعودية مؤخراً لنفي اختراق موقعها الخاص بشؤون المعلمين

وبدأت السعودية بالتفكير فى تطبيق قانون الحبس في جرائم الإنترنت عندما أعلنت السلطات هناك أنها ستفرض عقوبات بالحبس لمدة عام واحد وغرامات لا تزيد عن 500 ألف ريال لجرائم القرصنة المرتبطة بالإنترنت وإساءة استخدام كاميرات الهواتف المحمولة مثل التقاط صور من دون تصريح.

الجدير بالذكر، أن هيئة الأمر بالمعروف والنهي عن المنكر في السعودية، قد عارضت الهواتف ذات الكاميرات، وحظرت السعودية بيع هذه الأجهزة لعدة أشهر عام 2004، غير أن تلك القيود فشلت في وقف انتشار أحدث الصيحات التكنولوجية في البلد الذي يقطنه 24 مليون نسمة غالبيتهم من صغار السن ويتمتعون بمعدلات دخول فردية مرتفعة.

وتفرض السعودية رقابة شديدة على استخدام الإنترنت من خلال تعقب المستخدمين وحظر المواقع الجنسية وبعض المواقع ذات المحتوى السياسي. فبعد ازدياد الخطر من استخدام الإنترنت بادر العديد من المنظمات والهيئات إلى إطلاق الدعوات والتحذيرات من خطورة هذه الظاهرة التي تهدد كل مستخدمي الإنترنت، خصوصاً بعد تقرير برلماني وضعته لجنة العلوم والتكنولوجيا في مجلس اللوردات البريطانى أظهر أن شبكة الإنترنت تحولت إلى حلبة يرتع فيها المجرمون، وتنفذ فيها العصابات عمليات سرقة الأموال من الحسابات المصرفية، محذراً الحكومات والمؤسسات والشركات المختصة من عدم التدخل لتنظيم عملها قبل فوات الأوان.

ومن المفيد فى هذا الصدد، التأكيد على أن اقتصاد الظل الخفي يزداد انتعاشاً بفضل الجرائم الإلكترونية التي تدفع إلى الإحساس بأن الإنترنت تحول إلى منطقة شبيهة بـ «الغرب المتوحش» في أمريكا في عهودها الأولى، حيث تنعدم سيادة القانون.

ومن المخاطر الكبيرة أن المصارف حول العالم فقدت ملايين الجنيهات الاسترلينية، بسبب الاحتيال المصرفي، منها مبالغ خسرتها المصارف البريطانية عام 2010 والتى وصلت إلى أكثر من 67 مليون دولار.

وفى هذا الصدد، اقترح الباحثون إنشاء شرطة معنية بالمعلومات والإنترنت في السعودية، تحت مسمى «شرطة الإنترنت»، تكون مهامها تطهير

الإنترنت وحجب المواقع الإرهابية والمواقع التي تعود بالضّرر على المجتمع، لافتة إلى أهمية إنشاء مجلس وطني للمعلوماتية والإنترنت لاقتراح القواعد والتشريعات الخاصة.

ولقد حققت تجربة شرطة الإنترنت نجاحاً كبيراً في دول كثيرة مثل الصين وأمريكا ومؤخراً دولة فيتنام، ما يعزز مقترحا آخر يمثل إنشاء مجلس وطني للمعلوماتية والإنترنت له سلطة تقنية وأمنية ويكون من ضمن مسؤولياته اقتراح القواعد والتشريعات الخاصة بالمعلوماتية والإنترنت.

ومما يعزز ضرورات إنشاء هذا المجلس أنه سيكون من بين مسؤولياته، إعداد تقارير إحصائية ومتابعة ما تمّ عالمياً، واستقبال الشكاوى من الأفراد والمؤسسات وإرسالها إلى إدارة الاتصال في الشرطة الدولية، ووضع معايير للسياسات الوطنية، وتحديد المسؤولية بين الجهات ووضع تعريفات محددة لجميع لمصطلحات الإرهاب وتقنية المعلومات كافةً.

هذا ويتضمن النظام السعودي في قوانينه جريمة إنشاء موقع إرهابي على الإنترنت وفقاً للمادة السابعة من نظام مكافحة جرائم المعلوماتية، على أنه «يعاقب بالسجن مدة لا تزيد على 10 سنوات وبغرامة لا تزيد على 5 ملايين ريال، أو بإحدى العقوبتين، كل شخص يرتكب أياً من الجرائم المعلوماتية التي تتضمن إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، والدخول غير المشروع إلى الموقع الإلكتروني أو النظام المعلوماتي».

ومما يستلزم التأكيد عليه، ضرورة التدخل لمواجهة القصور في التشريعات والقوانين الحالية، أو تحديثها بالنصّ صراحةً على تجريم استخدام التقنيات العلمية الحديثة بالإضرار بأمن الدولة من الداخل والخارج، والسعي إلى وضع قانون للإنترنت يشتمل في أحد جوانبه على جرائم الإنترنت بشقيها الموضوعي والإجرائي، فضلاً عن ضرورة إنشاء منظمة عربية لتنسيق أعمال

مكافحة الإرهاب عبر الإنترنت وتشجيع قيام اتحادات عربية تسعى للتصدي لمثل تلك الجرائم، وكذلك تفعيل دور المنظمات والإدارات والحكومات العربية في مواجهة تلك الجرائم عبر نظام الأمن الوقائي.

وفى سبيل تفعيل آليات العمل والتعاون الدولي فى مجال مكافحة الجرائم الإلكترونية، فإنه من الأهمية بمكان التنسيق وتبادل المعلومات والخبرات مع الأجهزة المعنية بمكافحة الإرهاب عبر الإنترنت في دول العالم كافة، ونقل التقنية التي تستخدم في الدول المتقدمة في مكافحة الإرهاب الإلكتروني، والتوسع في دراسة فكر التنظيمات الإرهابية التي تبث عبر شركة الإنترنت، وتعزيز التعاون مع المؤسسات الدولية المعنية بخاصة «الإنتربول» لمواجهة جميع أشكال الجرائم، إضافة إلى الإسراع في الانضمام إلى المعاهدات الدولية الخاصة بمكافحة جرائم الإنترنت[1].

## ثانياً: مملكة البحرين

لا توجد قوانين خاصة بجرائم الإنترنت، وإن وجد نص قريب من الفعل المرتكب فإن العقوبة المنصوص عليها لا تتلاءم وحجم الأضرار المترتبة على جريمة الإنترنت.

## ثالثاً: سلطنة عمان

أصدرت السلطنة المرسوم السلطاني رقم 72/ 2001 الذي تضمن جرائم الحاسب الآلي وحدد فيه الجرائم التالية:

- الالتقاط غير المشروع للمعلومات أو البيانات.
- الدخول غير المشروع على أنظمة الحاسب الآلي.

---

(1) جريدة الشرق الأوسط 4 يوليو/ تموز 2010.

- التجسس والتنصّت على البيانات والمعلومات.
- انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم وتزوير البيانات أو وثائق مبرمجة أياً كان شكلها.
- إتلاف ومحو البيانات والمعلومات.
- جمع المعلومات والبيانات وإعادة استخدامها.
- تسريب البيانات والمعلومات.
- نشر واستخدام برامج الحاسب الآلي بما يشكل انتهاكاً لقوانين حقوق المِلْكية والأسرار التجارية..

## رابعاً: فلسطين

لا يوجد تشريع خاص يتعلق بجرائم الكمبيوتر والإنترنت إلا أنه يمكن ملاحقة هذه الجرائم عن طريق تطويع نصوص قانون العقوبات الفلسطيني بحيث ينطوي تحت لوائها بعض الجرائم المتعلقة بالكمبيوتر، كنصوص جرائم السرقة والنصب وخيانة الأمانة والإتلاف وغيرها. ولكن يهمنا أن نشير إلى أهمية التطور التشريعي لتحديد ماهية السياسة الجنائية الواجب اتباعها وفقاً للقانون الأساسي المعدل 2003م، والذي اشتمل على الضمانات الدستورية الخاصة بمكافحة الجريمة ومن بينها أنه لا جريمةَ ولا عقوبةَ إلا بنص قانوني، ولا توقع عقوبة إلا بحكم قضائي، ولذلك فقد استطاعت السلطة الوطنية في فترة وجيزة من الزمن، إصدار حزمة من التشريعات القضائية المتطورة منها قانون السلطة القضائية، وفانون الإجراءات الجزائية، وقانون الإجراءات المدنية والتجارية، وما زالت هناك مجموعة من التشريعات الجنائية المهمة قَيْد الإجراء في المجلس التشريعي من بينها مشروع قانون العقوبات والذي تعرض وبشكل مباشر في المواد(393 ـ 397) من الفصل السادس منه لجرائم الحاسب الآلي، وهناك مشروع قانون

الإنترنت والمعلوماتية، والذي لا يزال تحت الإعداد في ديوان الفتوى والتشريع بوزارة العدل، والذي تضمن العديد من القواعد والأحكام والجرائم والعقوبات المستحدثة فيما يتعلق بالإنترنت والمعلوماتية.

ويلاحظ أن قانون العقوبات الفلسطيني لسنة 1936 فيه من النصوص ما يتكفي لمعالجة جرائم الجنس عبر الإنترنت وإخضاعها للعقاب الجنائي خصوصاً في الفصل السابع عشر منه المتعلق بالجرائم التي تقع على الآداب العامة، وذلك وفقاً لأحكام المواد من 151 إلى 169 من القانون، كما أولى المشرِّع الجنائي الفلسطيني عناية وأهمية لهذه الجرائم في مشروع قانون العقوبات، والذي خصص له الفصل الثامن بعنوان (البغاء وإفساد الأخلاق)[1].

وبالرجوع إلى قانون العقوبات الفلسطيني لسنة 1936 فانه يمكن تعريف القَدْح وفقاً للمادة 201 منه على النحو التالي: (كل من نشر بواسطة الطبع أو الكتابة أو الرسم أو التصوير أو بأية واسطة أخرى غير مجرد الإيماء أو اللفظ أو الصوت وبوجه غير مشروع، مادةً تكون قذفاً بحق شخص، بقصد القذف بحق ذلك الشخص، يعتبر أنه ارتكب جنحة وتعرف تلك الجنحة بالقدح).

كما يعرّف القانون الذَمَّ في المادة 202 منه على النحو التالي(كل من نشر شفوياً وبوجه غير مشروع أمراً يكون قذفاً بحق شخص آخر قاصداً بذلك القذف في حق ذلك الشخص، يُعتبر أنه ارتكب جنحةً ويعاقب بالحبس مدة سنة واحدة وتعرف هذه الجنحة بالذم.

وتعرّف المادة 203 من القانون القذفَ على النحو التالي (تعتبر المادة مكونة قذفاً إذا أسند فيها إلى شخص ارتكاب جريمة أو سوء تصرف في وظيفة عامة أو أي أمر من شأنه أن يسيء إلى سمعته في مهنته أو صناعته أو وظيفته أو يعرضه إلى بغض الناس أو احتقارهم أو سخريتهم).

(1) راجع : قانون العقوبات الفلسطيني الصادر عام 1936.

إضافة إلى المواد المذكورة أعلاه، فان مشروع قانون العقوبات قد تضمن بين أحكامه هذه الجرائم حيث خصّص لها الفصل الرابع عشر منه بعنوان (الاعتداء على الشرف والاعتبار) وفقاً لأحكام المواد 323، 324، 325، 326، 327، 328، 329، 330، 331.

ومن جُماع هذه النصوص العِقابية يمكن توقيع عقوبة القذف والسبّ العلني أو غير العلني أو القذف بطريق الهاتف على من يقوم بإرسال شتائم إلى الغير بواسطة شبكة الإنترنت، وسواءٌ تمّ ذلك عن طريق إنشاء موقع خاص على شبكة الإنترنت لسبّ أو قذف شخص معين، أو سواء كان السَبُّ أو القذف عن طريق إرسال بريد إلكتروني للشخص المجني عليه.

وبالنسبة للتشريع الفلسطيني نجد أن القانون الأساسي المعدّل لسنة 2003 وقانون العقوبات يحميان الحياة الشخصية للمواطن من أي اعتداء عليها. فالمادة 32 من القانون الأساسي المعدل تنص على (كل اعتداء على أي من الحريات الشخصية أو حرمة الحياة الخاصة للإنسان وغيرها من الحقوق والحريات العامة التي يكفلها القانون الأساسي أو القانون، جريمةٌ لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وتضمن السلطة الوطنية تعويضاً عادلاً لمن وقع عليه الضرر. هذا وقد عالج قانون العقوبات لسنة 1936 هذه الجرائم في الفصل الثامن والعشرين منه، والذي جاء بعنوان الجرائم التي تقع على الحرية الشخصية. إضافة إلى ذلك، فان مشروع قانون العقوبات الذي لا يزال تحت الإجراء خصص الفصل الحادي عشر منه إلى جرائم الاعتداء على الحرية الشخصية والحياة الخاصة، وذلك وفقاً لأحكام المواد (300، 301، 302، 303، 304، 305، 306، 307، 308، 309، 310، 311، 312، 313، 314).

ونشير هنا إلى المادة 309 منه التي تنصّ على ((يُعاقب بالحبس مدةً لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة لأحد الأشخاص، بأن

ارتكب أحد الأفعال الآتية في غير الأحوال المُصرّح بها قانوناً أو بغير رضاء المَجنيّ عليه:

أولاً: استَرَقَ السمع أو سجّل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه، حديثاً خاصاً جرى في أحد الأماكن أو عن طريق الهاتف.

ثانياً: التقط أو نقل أو نسخ أو أرسل بأي جهاز من الأجهزة صورة شخص في مكان خاص، وإذا صدرت الأفعال المشار إليها أثناء اجتماع على مسمع ومرأى الأشخاص الذين يهمهم الأمر الحاضرين في ذلك الاجتماع، فان رضاء هؤلاء يكون مفترضاً ما لم يبدوا اعتراضهم على الفعل.

ثالثاً: أساء عمداً استعمال أجهزة الخطوط الهاتفية، بأن أزعج الغير أو وجه إليهم ألفاظاً بذيئة أو مُخِّلة بالحياء، أو تضمن حديثه معهم تحريضاً على الفسق والفجور.

## خامساً: الإمارات العربية المتحدة

شهدت دولة الإمارات في السنوات الأخيرة ثورة اقتصاديه وتقنيه هائلة، وتطورت فيها الأعمال بشكل ملحوظ، وأصبحت، بحسب تصنيف الكثير من الجهات العالمية والعربية، من أكثر الدول العربية في مجال استخدام الحاسب الآلي وشبكة الإنترنت.

وقد قطعت دولة الإمارات العربية المتحدة شوطاً كبيراً في مجال تكنولوجيا المعلومات من خلال إقامتها مدينة الإنترنت، وسعيها إلى رفع نسبة استخدام الشبكة الإليكترونية بين سكانها إلى 38٪ مع مطلع عام 2005، في وقت لا تتعدى فيه نسبة الحاسبات الشخصية في سوريا 1,6 ٪ بالنسبة لكل 100 ساكن أو 36 مستعملاً للإنترنت من بين كل عشرة آلاف مواطن، بالنظر إلى كل هذا يتضح عمق الهوة الرقمية في العالم العربي.

هذا وتتصدر الإمارات العربية المتحدة الدول العربية من حيث نسبة

مستخدمي الإنترنت من بين سكانها، حيث بلغت لديها 29،9٪، لتتبعها البحرين بنسبة 18،17٪، ثم قطر بنسبة 12،18 ٪، فالكويت بنسبة 11،29٪. على حين يقف في آخر القائمة العراق بنسبة 0،08٪، وقبله. السودان بـ 10،10٪

وإذا كان هذا هو موقع دولة الأمارات في خارطة استخدام الحاسب الآلي وتقنيات الاتصال الحديثة، فإنه من الطبيعي أن تكون الدولة مطمعاً لذوي النفوس الضعيفة من طالبي الثراء السريع، الذين يبحثون عن المال من مصادره غير المشروعة، أو من أولئك الأشخاص الذين سخروا طاقاتهم الذهنيه لا لاكتشاف النافع المفيد، وانما لإشباع غرور الذات لديهم وذلك من خلال محاولة الوصول الي أنظمة المعلومات، في الشركات والبنوك والمؤسسات، أو المنازل بدون وجه حق، بقصد الإفساد والتخريب، أو لمجرد العبث والمتعة، وهم المسمّون باسم (الهاكرز).

ناهيك عن أولئك الذين وجدوا في الحاسب الآلي وشبكة المعلومات بيئة خصبة لإرواء نزواتهم المنحرفة، والسعي لهدم قيم وأخلاق المجتمعات من خلال إنتاج وترويج البرامج الضارة بالفكر السليم والأخلاق والآداب السامية للمجتمع العربي المسلم.

**تشريعات مكافحة جرائم تقنية المعلومات**
**في دولة الإمارات العربية المتحدة:**

يعتبر قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم (2) لسنة 2006[1]، من أحدث التشريعات العربية في هذا المجال، والذي تم اقتراحه من قبل الدولة واعتماده لدى الأمانة العامة لمجلس التعاون لدول الخليج العربية كمسودة لمشروع قانون خليجي موحّد لمكافحة جرائم تقنية المعلومات، وتم

(1) راجع القانون الاتحادي رقم 2 لسنة 2006 بشأن مكافحة جرائم المعلومات، أبو ظبي 2006.

اعتماد صيغة المشروع في الاجتماع العاشر لوكلاء وزارات العدل في دول مجلس التعاون المنعقد بمدينة أبوظبي في شهر سبتمبر/ أيلول 2006.

على أنه من الضرورى أن نتعرف على القوانين الإماراتية فى مجال الاتصالات وتكنولوجيا المعلومات والتى كانت تعتبر نظيرَ آلياتِ الدولة الوطنية فى ملاحقة المجرم الإلكتروني، وفيما يلى بيان بهذه القوانين:

**نصوص قانون العقوبات الاتحادي رقم 3 لسنة 1987**

لقد وردت في قانون العقوبات، بحكم أنه القانون الجنائي العام، تقسيمات كثيرة للجرائم[1]، منها ما يقع على أمن الدولة الداخلي والخارجي، والجرائم الواقعة على الأموال (مثل جريمة السرقه، والنصب، وخيانة الأمانه والإتلاف)، والجرائم الواقعة على الأشخاص كالجرائم المتعلقه بحرمة الحياة الخاصة، والجرائم المتعلقة بالسمعة، والجرائم الماسّة بالآداب العامة، وجريمة التهديد)،والجرائم الماسة بالعقيدة والأديان، والجرائم الخاصة بوسائل المواصلات والاتصالات، وغيرها من الجرائم، وعلى ذلك فإن قانون العقوبات الاتحادي وإن كان لا توجد فيه نصوص خاصة لجرائم الحاسب الآلي، أو جرائم الشبكات، إلا أن العديد من الجرائم الواردة فيه، يمكن أن يستخدم الحاسب الآلي في ارتكابها كوسيلة أو أداة متمِّمة للجريمة، وتالياً، إذا تم في مرحلة التحقيق إدانة المتهم، والوصول إلى مرحلة إسناد التهمة إليه وفق نصوص قانون الإجراءات الجزائيه، وتحققت في حقه أركان الجريمه الموصوفه في قانون العقوبات الاتحادي فإنه سينال العقوبه الواردة في هذا القانون وبخاصة أن هناك مبدأً قانونياً مقرراً بالمادة (42) من قانون العقوبات نصّها (لا يعتبر الجهل بأحكام هذا القانون عذراً) هذه قاعده مَسَلّم بها في جميع التشريعات الجنائيه، ومن ثَمَّ لا يمكن لشخص ان يتعلّل بأنه لا يعلم أن مرتكب الجرائم عن طريق الحاسب

(1) راجع قانون العقوبات الاتحادي رقم 3 لسنة 1987، أبو ظبي 1987.

الآلي ليس مجرماً أو ليس له نصوص خاصة، مادام فعله يشكل جريمة تنطبق عليها أوصاف وأركان الجريمه الوارده بقانون العقوبات الاتحادي، وذلك تحقيقاً لمبدأ المشروعية، أو الشرعية الجنائية، ومقتضاه أنه لا جريمة ولا عقوبة إلا بنص، فحيثما وجد هذا النص سواء في قانون خاص أو عام، وارتكب شخص ما الفعل المحظور بموجب ذلك النص فإن الجريمه تقع، ويصبح من المشروع معاقبة مرتكبها، بغض النظر عن مسمى القانون، أو مكان ورود النص المُحرِّم للفعل.

ومن أمثلة الجرائم التي يمكن ان ترتكب عن طريق أجهزة الحاسب الآلي والأجهزة المرتبطة بها ويمكن معاقبة مرتكبيها بالعقوبات الوارده في قانون العقوبات الاتحادي، الجرائم الآتيه:

**1 ـ جريمة تخريب أو تعطيل وسائل الاتصال الدولية**

حيث نصّت المادة (21) على أنه ((يسري هذا القانون على كل من وجِدَ في الدولة بعد ان ارتكب في الخارج بوصفه فاعلاً أو شريكاً في جريمة تخريب أو تعطيل وسائل الاتصال الدوليه أو جرائم الاتجار بالمخدرات أو في النساء أو الصغار أو الرقيق أو جرائم القرصنة، والإرهاب الدولي)).

ولا شكّ أن مدلول عبارة ـ وسائل الاتصال الدولية ـ يشمل شبكة الإنترنت العالمية، وبذلك يكون القانون قد أخذ بمبدأ التضامن الدولي لمكافحة الجرائم عابرة الحدود، والجرائم المنظمة، وهذا النص يعتبر من النصوص الفريدة في قانون العقوبات، والذي صدر في عام 1987، وعليه فإنه بموجب هذا النص يمكن معاقبة من يعطل عمل شبكة (الإنترنت) بأية وسيله ـ كزرع الفيروسات مثلاً -، ولو لم يكن فعله قد تم في الدوله، فإنه يمكن ملاحقته إذا وجد في الدولة بموجب هذا النص، وتقديمه للمحاكمة ليأخذ جزاءه العادل بشرط ألا يكون قد تمت محاكمته في مكان آخر عن هذه الجريمه.

**2 ـ جريمة التهديد**

من المتصوَّر أن تتم جريمة التهديد المنصوص عليها في القانون عن طريق الحاسب الآلي، وذلك عن طريق كتابة التهديد في برنامج معين أو نشره على صفحة الويب، أو إرسال تهديد برسالة إلكترونية (إميل)، أو أثناء المحادثة التي تتم في غرف الدردشه (الشات) أو المنتديات، أو غرف المحادثة (البالتوك)، كما نصت المادة (351) من قانون العقوبات على أنه (يعاقب بالسجن مدة لا تزيد على سبع سنوات من هدّد آخرَ بارتكاب جناية ضد نفسه أو ماله أو ضد أو مال غيره أو بإسناد أمور خادشةٍ بالشرف أو إفشائها، وكان ذلك مصحوباً بطلب أو بتكليف بأمرٍ أو الامتناع عن فعلٍ أو مقصود به ذلك)).

على أنه ورد النصّ على التهديد البسيط في المادة (352) وهو التهديد الذي لا يصحبه طلب أو تكليف بأمر أو امتناع، وعاقب على هذا النوع بالحبس.

والملاحظ في هذين النّصين أن القانون لم يورد النصّ على وسيلة التهديد هل هي الكتابة، أو المُشافَهة، على عكس ماورد في نص قانون العقوبات المصري، مثلاً. وعليه فإن التهديد يقع بأية وسيله يتم بها وصوله إلى علم المجنيّ عليه، ومنها الوسائل التقنية الحديثة، وقد صدرت في بعض الدول أحكاماً بتطبيق قانون العقوبات على جريمة التهديد عن طريق الإنترنت.

**3 ـ جريمة تعطيل أو إتلاف وسائل الاتصالات السلكيه واللاسلكيه**

نظراً لأهمية وسائل الاتصالات السلكية واللاسلكية الحديثة في الحياة، ولأنها أصبحت شرياناً رئيسياً في جسم المجتمع النابض بالحركة والنشاط والتطور، وأصبحت هذه الوسائل عليها مدار التواصل الشخصي، والاقتصادي، والأمني، والعلمي، والتجاري، وعليها تتوقف حياة أشخاص وموتهم، وبتعطلها قد تتكبد الشركات، والدول، والأفراد خسائر جمّة تصل إلى المليارات، فإن المشرِّع أَوْلاها الاهتمام اللائق، وجرِّم كل اعتداء عليها يؤدي إلى تعطيلها، أو الإضرار بها.

ولا شك أنه يدخل في عمومية هذا النص، الاتصال والتواصل عبر شبكات الإنترنت الداخلية، أو العالمية، فهي وسيلة اتصالات لاسلكية، أضحت أكثر أهمية وأكبر أثراً في الحياة من الهاتف أو الفاكس والبرق، فإذا انصبّت الجريمة على تعطيل الشبكة المخصصة لمنفعة عامة فإن نص المادة التالية يمكن تطبيقه على هذه الجريمة بحيث ينال الجاني جزاءه العادل.

وفى هذا الصدد، ورد النص في المادة (279) عقوبات على أنه (يعاقب بالسجن مدة لا تزيد على عشر سنوات كل من عطل عمداً وسيلةً من وسائل الاتصال السلكية، واللاسلكية المخصصة لمنفعة عامة، أو قطع أو أتلف شيئاً من أسلاكها أو أجهزتها أو حالَ عمداً دون إصلاحها، وتكون العقوبه السجن مدةً لا تقل عن خمس سنوات إذا ارتكب الجريمه في وقت حربٍ أو فتنةٍ أو هياجٍ أو باستعمال مواد مفرقعة أو متفجرة).

**4 ـ الجرائم الماسّة بالآداب العامة**

اهتمّ المشرّع الإماراتي بحماية الآداب العامة في المجتمع حفاظا على المبادئ والقيم الإسلامية والعربية الأصيلة من العبث، وحفاظا على طهارة المجتمع وسموّ أخلاقه، وحفاظاً على أبنائه من العادات الدخيلة التي تصرف العقول والطاقات عن الإبداع والعطاء المفيد إلى الخنوع والجري وراء السراب المُلهي، والملذات الفانية. وإذا كانت جرائم الإخلال بالآداب العامة لها صور كثيرة وحسب المشرّع أنه عالج ما شاع منها وظهر واستشرى واشتهر، ووصل إلى حد المساس بقيم المجتمع، والنظام العام فيه. وعلى ذلك كان لظهور وسائل تقنية المعلومات الحديثة، وشيوع شبكة الإنترنت، وكسرها لحواجز الحدود بين الدول، وتسلقها لجدران الستر بين البيوت والمساكن، أثر كبير في شيوع جرائم الإخلال بالآداب العامة، لأن أصحاب النفوس الضعيفة، وعصابات الترويج للجنس المبتذل، والفجور وإفساد الأخلاق، وجدت في هذه الأجهزة الحديثة، وشبكات الإنترنت، بيئة خصبة للترويج لأنشطتها وترويج

بضائعها الفاسدة القبيحة، حتى أضحت المواقع، والصفحات التي تبث مواد مقروءةً، أو صوراً، ومقاطع أفلام، أو رسومات تتعلق بالجنس والممارسات الشاذة، تعد بعشرات الملايين، ناهيك عن تجارة الرقيق الأبيض، وجرائم استغلال الأطفال والنساء في الأمور المخلّة بالآداب.

وليس بخافٍ أن دولة الإمارات ـ في السنوات الأخيرة ـ قد شهدت بعض نماذج لجرائم مخلة بالآداب العامة، مثل تصوير فتيات وبثّ صورهن على شبكة الأنترنت، أو سرقة صور مخزنة في حاسبات شخصية وإعادة بثها بعد التلاعب بها ووضعها بمواقع تبث صوراً إباحية، ناهيك عن استخدام الهواتف الجوّالة المزودة بكاميرات، لتصوير الأشخاص بدون رضاهم وبثها على الملأ أو تصوير مشاهد مخلة بالآداب أو ممارسات شاذة وبث تلك الصور عبر الشبكة العالمية أو عن طريق خاصية التراسل بين الهواتف بتقنية (البلوتوث) أو غيرها من الطرق وبشكل عشوائي.

ومن جرائم الإخلال بالآداب والتحريض على الفجور والتي وردت في مواد القانون الإماراتى مايلي:

**أ ـ الجهر بما يخالف الآداب، أو إغراء الغير علانيةً بالفجور**

ورد النص على هذه الجرائم في المادة (361)، حيث نصّت على (يعاقب بالحبس مدة لا تزيد على ستة شهور وبغرامة لا تزيد على خمسة آلاف درهم أو بإحدى هاتين العقوبتين، كل من جهر بنداءٍ أو أغانٍ أو صدر عنه صياحٌ لأي خطاب مخالف للآداب وكل من جهر علانية بالفجور بأية وسيلة كانت).

ولعلّ المعوّل عليه في هذا النص بصدد الجرائم محلّ البحث، هو الجهر علانيةً بما فيه مخالف للآداب العامة، والأمر الثاني هو إغراء الغير بالفجور بأية وسيلة كانت، والعلانية، حسب ما وضحها شُرّاح القانون.

على أن العلنية تتحقق هنا بصدور النداء أو الصياح أو الغناء أو الخطاب المخالف للآداب في مكان عام أو خاص، طالما أن هناك أشخاصاً يسمعون ما

يجهر به الفاعل، لأن الغرض هو حماية الجمهور من كل ما يخدش كرامتهم وإحساسهم.

وفي مجال الإغراء الذي هو إغواء المجني عليهم وتحبيذ الفجور وتسهيل أمره لهم، اشترط القانون العلنية ولم يقيد الوسيلة، وباستخدام شبكة الإنترنت لإتيان هذه الأفعال المُجرّمة قانوناً من قبل الجاني، فإن تطبيق نص هذه المادة على الجريمة والجاني يصبح أمراً يسيراً ويحقق حماية في كثير من الحالات.

**ب ـ تجريم نشر وتوزيع وعرض الصور والأفلام والرسومات المخلّة بالآداب العامة**

أما المادة رقم (362) فقد جرّمت وعاقبت بالعقوبة ذاتها الواردة في المادة (361) المشار إليها سالفاً، حيث نصت على (كل من صنع أو استورد أو صدّر أو حاز أو أحرز أو نقل بقصد الاستغلال أو التوزيع أو العرض على الغير كتابات أو رسومات أو صوراً، أو أفلاماً أو رموزاً أو غير ذلك من الأشياء إذا كانت مخلة بالآداب العامة. ويعاقب بالعقوبة ذاتها كل من أعلن عن شيء من الأشياء المذكورة)، فهي إذن خمسة أفعال مختلفة، جرَّمتها المادة ولكن بشرط خاص ألا وهو اتجاه قصد الجاني إلى استغلالها أو توزيعها أو عرضها على الغير.

**قانون مؤسسة الإمارات للاتصالات رقم 1 لسنة 1991**

يُنظر إلى هذا القانون باعتباره القانون الأول المنظم لشؤون الاتصالات السلكية واللاسلكية في الإمارات، قبل صدور قانون تنظيم قطاع الاتصالات رقم (3) لسنة 2003[1]، وقد أنشأ هذا القانون مؤسسة الإمارات للاتصالات وحدد أهداف المؤسسة وأغراضها واختصاصاتها، وأعطى القانون المؤسسة دون غيرها حق نقل الاتصالات السلكية واللاسلكية وتشغيل وصيانة وتطوير نظام

(1) أنظر: قانون مؤسسة الإمارات للاتصالات رقم 1 لسنة 1991 وكذا قانون تنظيم قطاع الاتصالات رقم (3) لسنة 2003.

الاتصالات العامة بأسْرِه في الدولة، وكذلك بين الدولة والخارج وفقا لأحكامه، ونظّم هذا القانون حيازة واستعمال أجهزة الاتصالات وتراخيص الحيازة والاستعمال، وحدد شروط ومقابل الخدمات التي تقدمها المؤسسة، وذلك بموجب عقود تبرمها مع المنتفعين، وغيرها من الأحكام اللازمة، واشتمل القانون في الفصل السادس عشر منه على العقوبات التي توقع على مخالفة أحكامه، حيث وردت فيه عدة مواد تتضمن تجريماً لبعض الأفعال والعقوبات المقررة للجريمة؛ فالمادة الأولى مثلاً هي مادة عقابية عامة برقم (45) نصها الآتي: (مع عدم الإخلال بأية عقوبة أشد ينص عليها قانون آخر يعاقب كل من يخالف أحكام هذا القانون بغرامة لاتزيد على عشرة آلاف درهم (10000).

والمادة الثانية برقم (46) نصّها الآتي (يعاقب بالحبس لمدة لاتزيد عن ستة أشهر أو بالغرامة التي لاتزيد عن عشرة آلاف درهم:ـ

أ ـ كل من يختلس أو يسرق أو يحول أو يقوم بغير وجه حق باستغلال أو استعمال أي خدمة هاتفية أو أي تيار أو خِلافه مما قد يستعمل لتوصيل أو نقل الخدمات الهاتفيه أو غيرها من خدمات الاتصالات.

ب ـ كل من يستغل الأجهزة أو الخدمات أو التسهيلات التي تقدمها المؤسسة في الإساءة أو الأزعاج أو إيذاء مشاعر الآخرين أو أي غرض آخر غير مشروع.

ويجوز للمؤسسة ودون إذن مسبق، أن تضع تحت المراقبة أي جهاز أو خِلافه إذا توفرت لديها أسباب معقولة للاعتقاد بأنه يستغل في أي مخالفة من المخالفات المنصوص عليها في البند (أ) من هذه المادة أو بناءً على طلب المتضررين المشار اليهم في البند (ب) من هذه المادة.

وفي جميع الأحوال (لا يجوز للمؤسسة التنصّت على محتوى أو مضمون المكالمات دون إذن مسبق من السلطات القضائية المختصة). وقد أجمع رجال القانون والقضاء فى الإمارات على أن هذا القانون الخاص بمؤسسة الإمارات للاتصالات ـ وبما حواه من نصوص تجريمية- هو القانون المعوّل عليه في

ملاحقة الجرائم التي ارتكبت عبر شبكة الإنترنت للوصول إلي أجهزة الحاسوب الشخصية أو التابعة للمؤسسات أو البنوك والشركات خلال الأعوام المنصرمة، وذلك لأن خدمة الإنترنت تعتبر من الخدمات التي تقدمها مؤسسة الإمارات للاتصالات بموجب عقد بينها وبين المنتفعين، وعليه فإن أي اساءة أو استخدام غير مشروع لتلك الخدمة بالمخالفة لأحكام هذا القانون كانت تعطي للجهات الأمنية وجهات التحقيق القضائية (النيابة العامة) المُكْنةَ من تقديم المخالفين ومرتكبي الجرائم التقنية الحديثة إلى العدالة، استناداً لهذه المواد، وكذلك مواد قانون العقوبات الاتحادي على ما سنراه من خلال استعراضنا للجرائم التي تمّ ضبطها، في السنوات الأخيرة وتم تقديم مرتكبيها للعدالة، قبل صدور قانون مكافحة جرائم تقنية المعلومات في شهر يناير/ كانون الثاني 2006.

ولعلّ مما سهّل على جهات التحقيق تقديم مرتكبي جرائم تقنية المعلومات للعدالة استناداً لنصوص هذا القانون، الطريقة التي صيغت بها نصوص هذه المواد، فهي نصوص مرنة وفيها مترادفات عدة، وهي من العمومية بما جعل الاستناد إليها يسيراً في أغلب الأحيان وبخاصة إذا كانت الجريمة مرتكبة عن طريق استغلال شبكة الإنترنت التي تعتبر خدمة من خدمات الاتصالات، أو عن طريق استخدام أجهزة الاتصال الأخرى؛ ففي البند (أ) من المادة (46) المشار إليها وردت عبارة (أو غيرها من خدمات الاتصالات) بعد أن ذكر الخدمة الهاتفية أو أي تيار أو خلافه مما قد يستعمل لتوصيل أو نقل الخدمات الهاتفية. كما ورد في البند (ب) ألفاظ عامة ومترادفات شاملة تسهل على المحققين الاستعانة بالنص لتقديم كل من يرمي إلى غرضٍ غير مشروع أو إلى إيذاء الآخرين عن طريق استخدام خدمات مؤسسة الاتصالات؛ حيث جاء النص بلفظ (كل من يستغل الأجهزة أو الخدمات أو التسهيلات التي تقدمها المؤسسة في الإزعاج أو إيذاء مشاعر الآخرين أو أي غرض آخرغير مشروع) ليأتي بعد ذلك دور محكمة الموضوع لتكييف طبيعة العمل غير المشروع،

وطبيعة الإساءة التي ارتكبها الشخص الجاني، والمادة العقابية المنطبقة سواء من هذا القانون أو قانون العقوبات الاتحادي.

على أنه في كثير من الجرائم المرتبطة بالحاسب الآلي، لن يكون هذا القانون قادراً على أداء الغرض المطلوب، وسوف تقف الجهات الأمنية والمحققون مكتوفي الأيدي، في ظل عدم وجود قانون خاص بجرائم الحاسب الآلي أو جرائم تقنية المعلومات، وذلك ما سيتضح من خلال العرض الذي سوف نقدمه للجريمة التي نظرتها محاكم دبي، وكيف أن تطبيق هذا القانون وقانون العقوبات على الجريمة المُقدَّم مرتكبها للمحاكمة لم يكن من السهولة بمكان، وكيف أن القاضي اضطر للاجتهاد والقياس لتوسيع مفهوم النص الجنائي ليتمكن من إدانة المتهم، على الرغم من صعوبة ذلك القياس في مجال النص الجنائي، والمحاذير التي تحول دون ذلك الاجتهاد.

**قانون تنظيم قطاع الاتصالات رقم (3) لسنة 2003**

صدر قانون تنظيم قطاع الاتصالات ليكون القانون الذي ينظم عمل شركات الاتصالات في الدولة، وينشئ هيئة جديدة تسمى هيئة تنظيم قطاع الاتصالات بالدولة، وحُدّدت االمادة (12) من هذا القانون مهام وصلاحيات واختصاصات الهيئة بأنها هي السلطة المختصة بالرقابة على قطاع الاتصالات والمرخص لهم، وذلك وفقاً لأحكام هذا المرسوم بقانونٍ ولائحته التنفيذية والتعليمات الصادرة عن اللجنة العليا، . . . . إلخ).

وورد في المادة رقم (1) من القانون تعريف (لخدمات الاتصالات) بأنها خدمة نقل أو بث أو تحويل أو استقبال من خلال شبكة الاتصالات لأيّ مما يأتي:

الاتصالات السلكية واللاسلكية ـ الحديث والموسيقى وغيرها من الأصوات ـ الصور المرئية ـ الإشارات التي تستخدم في البث باستثناء البرامج

وإذاعتها ـ الإشارات المستخدمة في التشغيل والسيطرة على أي آلات أو أجهزة تركيب أو صيانة أو ضبط أو إصلاح أو تغيير أو نقل أو إزالة الأجهزة التي سيتم ربطها أو تكون مرتبطة بشبكة اتصالات عامة ـ إنشاء وصيانة وتشغيل شبكات البرق والهاتف والتلكس والدوائر المؤجرة والمعطيات المحلية والدولية والإنترنت والإرسال اللاسلكي ـ أي خدمات اتصالات تعتمدها اللجنة العليا.

وورد في الباب التاسع من هذا القانون مجموعة مواد تجرم بعض الأفعال وتفرض عقوبات على مخالفة الأحكام والالتزامات التي يفرضها القانون، حيث نصت المادة (71) على عقوبة الحبس مدة لا تجاوز سنتين، وبغرامة لا تقل عن خمسين ألف درهم ولا تجاوز مائتي ألف درهم أو بإحدى هاتين العقوبتين، كل من يباشر أياً من الأنشطة التي نظمها القانون من دون الحصول على ترخيص أو إعفاءٍ وفقاً لأحكام هذا القانون، أو يقوم متعمّداً بتغيير أو إتلاف أو إخفاء أية وثيقة أو معلومة تطلبها اللجنة العليا أو الهيئة أو لم يقم بتعديل أوضاعه وفقاً لأحكام هذا المرسوم بقانونٍ خلال المدة المحددة.

كما ورد في المادة رقم (72) تجريم بعض الأعمال التي يمكن أن تتم عن طريق الخدمات التي تقدمها شركات الاتصالات أو عن طريق أجهزة الاتصالات، حيث فرض القانون في هذه المادة عقوبة الحبس لمدة لا تجاوز سنة وبغرامة لا تقل عن خمسين ألف درهم ولا تجاوز مائتي ألف درهم أو بإحدى هاتين العقوبتين:

1 ـ كلَّ من أقدم أو ساهم في تقديم خدمات اتصالات مخالفة للنظام العام والآداب العامة.

2 ـ كلّ من استغل أجهزة أو خدمات الاتصالات في الإساءة أو الإزعاج أو إيذاء مشاعر الآخرين أو لغرض آخر غير مشروع.

3 ـ كلّ من نسخ أو أفشى أو وزع بدون وجه حق فحوى أي اتصال أو رسالة هاتفية مرسلة من خلال استخدام شبكة اتصالات عامة.

4 ـ كل من قام متعمداً بالدخول غير المشروع لشبكة اتصالات أو قام بتعطيل أي من خدمات الاتصالات.

5 ـ كل من استغلّ أو استخدم بغير وجه حق أيّاً من خدمات الاتصالات.

6 ـ كل من تنصّت على محتوى أو مضمون المكالمات دون إذن مسبق من السلطات القضائية المختصة.

بمتابعة وتمحيص النصوص التي تم استعراضها، فإنه يمكننا القول بأن بعض الجرائم التي يمكن أن تتم عن طريق استخدام شبكة الإنترنت يمكن ملاحقة مرتكبيها بموجب أحكام هذا القانون، حيث ورد النصّ على أن خدمة (الانترنت) تعتبر من (خدمات الاتصالات) الوارد تعريفها بالمادة الأولى.

كذلك ورد النص صراحة على جرائم محددة وهي(تقديم، أو المساهمة في تقديم خدمات اتصالات مخالفة للآداب العامة أو النظام العام)، ويندرج تحت هذا المصطلح العديد من الجرائم وبخاصة ترويج الصور والمواد الإباحية أو المشاهد الخادشة للحياء أو الدعوة للفجور والرذيلة أو الدعوة لتعكير صفو الأمن واشاعة الفوضى، أو تعكير أمن الناس وسكينتهم وتعريض صحتهم للخطر، وهذه الجرائم إذا ارتكبت عن طريق شبكة الإنترنت التي هي خدمة من خدمات الاتصالات فمثل هذه الجرائم يمكن ملاحقة مرتكبيها وفقاً لأحكام هذا القانون.

كذلك جريمة تعطيل عمل شبكة الإنترنت وهي من الجرائم الخطيرة والمؤثرة يمكن ملاحقة مرتكبيها بموجب نص المادة السابقة حيث ورد في البند رقم (4) النص صراحةً على تجريم تعطيل أيٍ من خدمات الاتصالات والتي من ضمنها خدمة الإنترنت.

وحيث أن هذا القانون أعطى الحق للهيئة بالفحص والتدقيق على الأجهزة المستخدمة لتقديم خدمات الاتصالات، فإن من يمتنع عن السماح للهيئة أو

للموظفين المختصين بالفحص والتدقيق على الأجهزة التي تكون تحت تصرفه أو الدخول لموقعه فسوف يعرض نفسه للعقوبة المقررة في المادة (74) من هذا المرسوم بقانون وهي الغرامة التي لا تقل عن خمسين ألف درهم ولا تجاوز مائتي ألف درهم. ولا شك أن أجهزة الحاسب الآلي المستخدمة في تلقي خدمة الإنترنت داخلةٌ ضمن حكم هذه المادة، ولذا يستطيع الموظفون المختصون ورجال التحقيق فحص أجهزة الحاسب الآلي التي يعتقدون أنها كانت محلاً لنشاط إجرامي بالمخالفة لأحكام هذا القانون والقوانين الأخرى النافذة في الدولة.

ولعله من الأهمية بمكان فى هذا الصدد وبعد استعراض النصوص التي يمكن من خلالها ملاحقة مرتكبي جرائم تقنية المعلومات في القانونين الخاصين بمؤسسة الإمارات للاتصالات، وتنظيم قطاع الاتصالات، أن نشير إلى أن القانون الثاني، وهو قانون تنظيم قطاع الاتصالات الصادر في عام 2003 يعتبر معدِّلاً لقانون مؤسسة الإمارات للاتصالات، حيث ورد النص صراحة فيه على إلغاء بعض المواد ومن ضمنها المواد الخاصة بالعقوبات، وأصبحت المواد الواردة بقانون تنظيم قطاع الاتصالات هي الواجبة التطبيق على جميع مسائل المخالفات والجرائم المرتكبة من خلال وسائل أو خدمات الاتصالات في الدولة فضلاً عن العقوبات الواردة في قانون العقوبات الاتحادي والقوانين الأخرى ذات الصلة.

## المبحث الثالث:
## القصور التشريعي ونمط تعاطي القضاء العربى مع جرائم المعلوماتية

### أوجه القصور التشريعي في الدول العربية

إذا حاولنا الوقوف على أوجه القصور التشريعي في كثير من الدول

العربية ، والتي تحول دون الملاحقة الجنائية لمرتكبي الجرائم المعلوماتية يمكننا أن نشير إلى ما يلي :

(1) إن مبدأ الشرعية الجنائية يفرض عدم جواز التجريم والعقاب عند انتفاء النص، الأمر الذي يمنع مجازاة مرتكبي السلوك الضارّ أو الخَطِر على المجتمع بوساطة الحاسوب (الكمبيوتر) أو الإنترنت ؛ طالما أن المشرّع الجنائي لم يقم بسنّ التشريعات اللازمة لإدخال هذا السلوك ضمن دائرة التجريم والعقاب.

ولذا يتعين على المشرعين في سائر الدول العربية مواكبة التطورات التي حدثت في المجمعات العربية ؛ وسن التشريعات اللازمة للتصدي لظاهرة الإجرام المعلوماتي.

وهنا تجدر الإشارة إلى أن المشرع العُماني كان له قصب السبق في هذا المضمار ؛ حيث نصّ على تجريم كثير من صور الجرائم المعلوماتية.

(2) يعتبر مبدأ الإقليمية هو المبدأ المهيمن على تطبيق القانون الجنائي من حيث المكان، غير أن هذا المبدأ يفقد صلاحيته للتطبيق بالنسبة للجرائم المعلوماتية، التي تتجاوز حدود المكان، فجرائم الإنترنت عابرة للحدود.

(3) انعدام وجود تصوّر واضح المعالم للقانون والقضاء تجاه جرائم الإنترنت لكونها من الجرائم الحديثة، وتلك مشكلة أكثر من كونها ظاهرة، ولانعدام وجود تقاليد بشأنها كما هو الشأن في الجرائم الأخرى، ويساعد على ذلك انعدام وجود مركزية وملكية عبر الإنترنت.

(4) رغم صدور عدد من التشريعات العربية بشأن حماية الملكية الفكرية والصناعية التي تضمنت النصّ على برامج الحاسب واعتبرتها من ضمن المصنفات المحمية في القانون ؛ إلا أن مكافحة الجرائم المعلوماتية في

الدول العربية ما زالت بلا غطاء تشريعي يحدِّدها ويجرِّم صورها كافة بخلاف بعض الاستثناءات. وإذا كانت التشريعات العربية ـ فى الغالب الأعم ـ قاصرة في مجال ملاحقة صور السلوك الضارّ والخَطِر المتعلقة باستخدام الحاسوب (الكمبيوتر) والإنترنت؛ فإن هذا القصور انعكس مردوده على الجانب الإجرائي المتعلق بمكافحة الإجرام المعلوماتي، فلم تصدر تشريعات جنائية إجرائية كافية لتعقب مقترفي هذا الإجرام.

(5) تتعدد مظاهر القصور التشريعي التي يتعين أن تواجه مظاهر السلوك السلبي المتعلقة بتقنية المعلومات كافة. فالتشريعات ما زالت ناقصة وقاصرة في المجالات التالية:

- التشريعات الخاصة بالملكية الفكرية فيما يتعلق بأسماء مواقع الإنترنت وعناصرها ومحتواها، والنشر الإلكتروني، وفي حقل التنظيم الصحفي للنشر الإلكتروني.
- تنظيم التجارة الإلكترونية والتشريعات الضريبية التي تغطي الميادين الخاصة بالضريبة في ميدان صناعة البرمجيات والأعمال على الإنترنت والتجارة الإلكترونية.
- مقاييس إطلاق التقنية.
- القواعد التشريعية لنقل التكنولوجيا.
- التراخيص والاستثمار والضرائب المتعلقة بتكنولوجيا المعلومات.
- تنظيم حجية ومقبولية مستخرجات الحاسب.
- وسائل الإثبات التقنية والإثبات المدني.
- وتنظيم الصور الإجرامية في ميدان الحاسب والإنترنت.
- أنظمة الدفع النقدي الإلكتروني.

- تنظيم كيفيّة عمل مقاهي الإنترنت.
- البرمجيات الصناعية.

(5) عدم الاهتمام بالتفتيش على أجهزة الحاسوب (الكمبيوتر)، فالتشريعات العربية ـ في مجملها ـ لم تحدد قواعد خاصة للتفتيش على الحاسبات الآلية وكيفية ضبط المعلومات التي تحويها، ومراقبة المعلومات أثناء انتقالها، كما أن الإجراءات الجنائية للجهات القائمة على التفتيش غير حاسمة بشأن مسألة ضبط برامج الحاسب والمعلومات الموجودة في الأجهزة وفقاً للشروط الخاصة بإجراءات التفتيش العادية.

(6) إذا كان المحقق مهمته البحث عن الحقيقة، وإذا كان القاضي مهمته هي الفصل فيما يعرض عليه من أقضية ومنازعات، فإن عمل المحقق وعمل القاضي يحتاج كلٌّ منهما إلى بيئة قانونية تساعدهما على أداء وظيفتيهما.

الشيء المؤسف أن هذه البيئة القانونية إما غامضة ؛ وإما قاصرة.

ففيما يتعلق بمواطن القصور والغموض، فهى متعددة، ونستلهمها من التساؤلات الآتية:

- هل اعتداءات الأشخاص على الأموال في البيئة الحقيقية يمكن تطبيق مفهومها على اعتداءات المجرم المعلوماتي ؟
- هل المعلومات بذاتها لها قيمة مالية ؟ أم هي تكون كذلك عندما تمثل أصولاً أو حقوقاً؟.
- كيف يمكن حماية السر التجاري أو الأسرار الشخصية وبيانات الحياة الخاصة من اعتداءات المجرم المعلوماتي أو المتطفل دونما تصريح وإذن ؟.
- وهل هناك معايير تحكم مقدمي خدمات الإنترنت بأنواعها ؟.
- ما مدى المسؤولية القانونية في حالة تحميل الملفات الموسيقية من

الإنترنت بغير موافقة صاحب الموقع ؟ .

- هل يعتبر النشر الإلكتروني على الإنترنت من قبيل النشر الصحفي المنظم في تشريعات الصحافة والمطبوعات ؟ .
- وهل إبرام العقد عبر الإنترنت تتوافر فيه سلامة وصحة التعبير عن الإرادة بالقدر ذاته الذي يوفره التعاقد الكتابي أو الشفهي في مجلس العقد العادي ؟
- وهل توقيع العقود والمراسلات إلكترونياً يتساوى مع توقيعها ورقياً ؟
- هل ما يُعتدّ به من دفوع واحتجاجات بشأن التزامات أطراف التعاقد أو علاقات الدفع التقليدية متاح بذاته أو أقل منه أو أكثر في البيئة الرقمية ؟
- هل لرسائل البريد الإلكتروني حجية في الإثبات ؟ وهل لها ذاتها قيمة المراسلات الورقية؟
- هل الانتخاب الإلكتروني هو تصويت صحيح ومقبول لمن اخترناه ممثلاً لنا في عالم المكان والجغرافيا؟ .
- هل العلامة التجارية محميةٌ من أن تكون اسماً ناطقاً لطرف آخر ؟
- ماذا عن تصميم الموقع؟ هل ثمة قدرة على منع الآخرين من سرقته واستخدامه؟
- ماذا إن تمّ ربط موقعك على الإنترنت مع موقع لا ترغب في أن يكون بينهما رابط ؟
- ماذا عن فرض المحتوى على المستخدم؛ هل يظل المستخدم عاجزاً لا حول له ولا قوة أمام تدفق مواد لا يرغبها أو لا يطلبها على صندوق بريده أو خلال تصفحه المواقع التي يريدها ؟
- هل إغلاق المواقع ذات المحتوى غير المشروع في بعض النظم

والمشروع في غيرها تجاوزٌ على ديمقراطية العالم التخيلي ؟

- متى نشأ النزاع أياً كان وصفه أو مصدره، فمن هو القاضي الرقمي ؟
- ما هو القانون الذي سيحكم النزاع ؟
- ما المحكمة ومن هو المحكَّم ؟
- ما هي أخلاق المجتمع الرقمي وقواعد السلوك فيه، هل هي ذاتها أخلاق العالم الحقيقي أم أنّ ثمة تبايناً في المفهوم والقيود ؟
- وهل ثمة قدرة للمستخدم، أن يطالب بحقوق في مواجهة الطرف الوسيط في كل تعامل أو استخدام نتج عنه مَساسٌ بحق من حقوقه.
- ومن هو حاكم الإنترنت وما الدستور الذي يحكمه، ومن هو الشرطي الذي يُهرَع له المستخدم إن تعرض لاعتداء سافر على حقوقه أو بياناته أو محتوى موقعه أو رسائله أو خصوصيته؟.
- كيفية حماية برامج الحاسب.
- كيفية مقاضاة مزودي خدمة الإنترنت على انقطاع الخدمة.
- مراقبة أداء الموظفين عبر البريد الإلكتروني ورسائلهم في بيئة العمل.
- مدى صحة إبرام العقد على الإنترنت.
- كيفية حماية مواقع الإنترنت.
- هل إرسال رسالة مُمازحةٍ عبر البريد الإلكتروني، يمكن ان تشكل جريمة جنائية ؟وهل يمكن أن ترتب مسؤولية مدنية ؟

## بواعث حتمية سد الفراغ التشريعي في مجال مكافحة الجرائم المعلوماتية فى الدول العربية

مما لاشك فيه أن أسباب سد الفراغ التشريعي في مجال مكافحة الجرائم

المعلوماتية متعددة ؛ وكلها تنبع من كون هذه الجرائم تختلف جملةً وتفصيلاً عن الجرائم العادية ؛ ولذا يتعين أن يكون تعقبها يراعي هذه الاختلافات.

وعلى كل حال، من أهم هذه الأسباب ما يلي :

**أولاً : سهولة إخفاء الجريمة**

الجريمة المعلوماتية ـ في أغلب الأحوال ـ تكون مستترة خفية؛ فعلى سبيل المثال نجد أن اختلاس المال بالتلاعب غير الشرعي ؛ غالباً ما يحاول المختلس تغطيته وستره والتجسس على ملفات البيانات المختزنة ؛ الأمر الذي يضعف إلى حد كبير فرصة المجني عليه في إثبات هذا الاختلاس.

**ثانياً: الشيء نفسه يقال بالنسبة لاختراق قواعد البيانات،** وتغيير بعض محتوياتها والتخريب المنطقي للأنظمة باستخدام الفيروسات.

**ثالثاً : نقص خبرة الشرطة وجهات الادعاء والقضاء.**

**رابعاً : صعوبة الوصول إلى مرتكبي أغلب الجرائم المعلوماتية :**

فعلى سبيل المثال : جرائم التزوير عبر الإنترنت تتم دون تحديد شخص مرتكبها أو ضبط المحرِّر المزوِّر.

**خامساً : صعوبة الإثبات**

وذلك يرجع إلى :

(1) الطبيعة الخاصة للدليل في الجرائم المعلوماتية، فهو ليس بدليل مرئي يمكن فهمه بمجرد القراءة، ويتمثل ـ حسب ما تتيحه النظم المعلوماتية من أدلة على الجرائم التي تقع عليها أو بواسطتها ـ في بيانات غير مرئية لا تفصح عن شخصية معينة عادة.

وتظهر هذه المشكلة بصفة خاصة بالنسبة لجرائم الإنترنت مثل الجرائم

التي ترتكز على البريد الإلكتروني في ارتكابها، إذ يكون من الصعب على جهات التحري تحديد مصدر المرسل.

(2) صعوبة الوصول إلى الدليل، وذلك نتيجة قيام كبرى المواقع العالمية على الإنترنت بإحاطة البيانات المخزنة على صفحاتها بسياج من الحماية الفنية لمنع التسلل للوصول غير المشروع إليها لتدميرها أو تبديلها أو الاطلاع عليها أو نسخها.

هذا من جهة؛ ومن جهة أخرى يمكن للمجرم زيادة صعوبة عملية ضبط أي دليل يدينه، وذلك من خلال: استخدامه كلمات مرور بعد تخريب الموقع مثلاً، أو استخدامه تقنيات التشفير.

(3) سهولة محو الدليل، فالجاني يستطيع أن يتوجه إلى أي «مقهى للإنترنت» والدخول على أحد المواقع وإرسال رسالة على البريد الإلكتروني لآخر تحوي عبارات سَبّ وقذف، ثم يقوم بمحو الدليل وإعادة كل شيء كما كان عليه والانصراف إلى حال سبيله.

(4) أدلة الإدانة ذات نوعية مختلفة فهي معنوية الطبيعة، وذلك مثل سجلات الكمبيوتر ومعلومات الدخول والاشتراك والنفاذ والبرمجيات، ولذا فهذه الأدلة تثير أمام القضاء مشكلات عديدة؛ ولاسيما فيما يتصل بمدى قبولها وحجيتها والمعايير اللازمة لذلك.

**سادساً: إحجام الجهات والأشخاص المجني عليهم عن الإبلاغ عن الجرائم المعلوماتية**

ويحدث ذلك غالباً بالنسبة للجهات المالية كالمصارف والبنوك ومؤسسات السمسرة؛ إذ أن مجالس إداراتها ـ في الغالب الأعم ـ تفضل كتمان هذه الجرائم تفادياً للآثار السلبية التي قد تنجم عن كشفها، أو اتخاذ الإجراءات القضائية تجاهها؛ إذ قد يؤدي ذلك إلى تضاؤل الثقة فيها من جانب المتعاملين معها.

**سابعاً : صعوبات شديدة في ضبط وتوصيف جرائم المعلوماتية**

لا مِراءَ في أن رجال الضابطة القضائية والمحققين والقضاة يصادفون صعوبات جمّة فيما يتعلق بإجراءات ضبط الجرائم المعلوماتية ؛ وإضفاء الوصف القانوني المناسب على الوقائع المتعلقة بهذه الجرائم.

ولعل مردّ ذلك يرجع إلى الطبيعة الخاصة لهذه الجرائم. فهي تتم في فضاء إلكتروني يتسم بالتغيير والديناميكية والانتشار الجغرافي عابر الحدود.

**ثامناً: تصادم التفتيش عن الأدلة في الجرائم المعلوماتية مع الحق في الخصوصية المعلوماتية**

وذلك لأن هذا التفتيش يتم ـ غالباً ـ على نظم الكمبيوتر وقواعد البيانات وشبكات المعلومات، الأمر الذي قد يتجاوز النظام المشتبه به إلى أنظمة أخرى مرتبطة ؛ نظراً لشيوع التشبيك بين الحواسيب وانتشار الشبكات الداخلية على مستوى المنشآت والشبكات المحلية والإقليمية والدولية على مستوى الدول.

ولاشك في أن امتداد التفتيش إلى نظم غير النظام محل الاشتباه، قد يمسّ ـ في الصميم ـ حقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش.

**تاسعاً : فكرة الاختصاص والطبيعة الدولية للجرائم المعلوماتية**

الجرائم المعلوماتية تتم ـ في الغالب الأعمّ ـ بأفعال ترتكب من قبل أشخاص من خارج الحدود كما أنها تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود، الأمر الذي

يثير التساؤل حول الإختصاص القضائي بهذه الجرائم ؛ علاوة على أن امتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود ؛ أمر يحتاج إلى تعاون دولي شامل يستهدف تحقيق مكافحة هذه الجرائم ؛ مع احترام السيادة الوطنية للدول المعنية.

## أمثلة تطبيقية لنمط تعاطى القضاء العربى مع الجرائم الإلكترونية

**1 ـ مثال تطبيقى من دولة الإمارات العربية المتحدة لجريمة إلكترونية نظرت أمام القضاء الوطني قبل صدور قانون مكافحة جرائم تقنية المعلومات:**

وقعت الجريمة عبر (شبكة الإنترنت) في دولة الإمارات قبل صدور قانون مكافحة جرائم تقنية المعلومات رقم 2 لسنة 2006، حيث تم القبض على مرتكبها وتقديمه للعدالة بموجب قانون العقوبات الاتحادي، وصدر حكم المحكمة الابتدائيه ببراءته من التهمة لعدم وجود نص واضح يجرّم الفعل الذي قام به، وفي محكمة الاستئناف تعدل الحكم إلى إدانة المتهم وتأيد الحكم من محكمة التمييز.

وتثور فى هذا الصدد عدة تساؤلات منها:

- لماذا لم تستطع المحكمة الابتدائية إدانة المتهم؟
- وكيف توصلت محكمة الاستئناف إلى إدانته ؟
- وماذا قالت محكمة التميز عن الحكم، وكيف بررت تأييدها له، في الرد على أوجه الطعن الموجّه له من الدفاع؟
- وكيف أوحت محكمة التمييز بأن هناك حاجة إلى نصوص قانونيه تعالج جرائم الحاسب الآلي الحديثة في الدولة؟

وللإجابة على هذه التساؤلات كان من المهم أن نستعرض هذه القضية ونسبر أغوارها في ما يلي:

1) **اتهمت النيابة العامة المدعو (. . . . .) في الجنحة رقم 5883/ 2000**، بأنه في يوم 21/ 6/ 2000، استغل وأساء استخدام خدمة من خدمات مؤسسة الإمارات للاتصالات (خدمة الإنترنت) وذلك لأغراض غير مشروعة، بأن زوّد الحاسب الآلي الذي يستخدمه والمتصل بهذه الخدمة ببرنامج قرصنة

تمكن من خلاله من كسر الكلمات السرية الخاصة ببعض موظفي مؤسسة الإمارات للاتصالات والدخول إلى الأماكن غير المصرح بها لمشتركي الشبكة ونسخ بعض الكلمات الخاصة بالكلمات السرية ورسائل البريد الإلكتروني لموظفي مؤسسة الإمارات للاتصالات مع علمه بذلك.

2) **فضَّ المتهم عدداً من الرسائل الواردة إلى بعض موظفي مؤسسة الإمارات للاتصالات والمسجلة على البريد الإلكتروني للمؤسسة**؛ وذلك بأن قام بكسر الكلمات التي تحول دون علم واطلاع الغير عليها ونسخ صوراً منها احتفظ بها على جهاز الحاسب الآلي الخاص به، وطلبت النيابة معاقبته طبقاً لنص المادة 46/ 7 من القانون رقم (1/ 91) في شأن مؤسسة الاتصالات والمادة 380 عقوبات، وادعت المؤسسة مدنياً قِبَلَ المتهم طالبة الحكم بإلزامه بمبلغ 2,835000 درهم على سبيل التعويض.

3) **وبتاريخ 1/ 7/ 2001 حكمت محكمة أول درجة ببراءة المتهم من التهمة الثانية**، وهي تهمة فض الرسائل المؤثَّمة بموجب قانون العقوبات، وكان سند البراءة أن القاضي الإبتدائي اعتبر أن الرسالة الإلكترونية الواردة بالإيميل، شي مغاير للرسالة العادية المكتوبة، وأن النص الجنائي فرض الحماية على هذه الأخيره فقط، ذلك أنه عندما صدر قانون العقوبات لم يكن هناك شي يسمى بالرسالة عبر الإيميل، وتحترز من استخدام القياس في مجال النص الجنائي التزاماً بقاعدة الشرعية الجنائية، ولعدم وجود مبادئ من المحكمة العليا في هذا الشأن.

وأدانت المحكمة المتهم عن التهمة الأولى وهي إساءة واستغلال خدمة من خدمات الاتصالات، وطبقت عليه العقوبة الواردة بقانون مؤسسة الاتصالات وقامت بتغريمه عشرة آلاف درهم عن هذه التهمة، وبإحالة الدعوى المدنية إلى المحكمة المدنية المختصة.

4) **لم يرتض المحكوم عليه والنيابة العامة الحكم، فطعنا عليه بالاستئناف،**

فحكمت الاستئناف بإلغاء ما قضى به الحكم المستأنف و القضاء مجدداً بتغريم المتهم عشرة آلاف درهم عن التهمتين المسندتين إليه مع مصادرة المضبوطات، بعد أن أعملت قواعد الارتباط بين التهمتين؛ أي أن محكمة الاستئناف أدانته عن تهمة فض الرسائل الإلكترونية وقاستها على الرسائل العادية، وتوسعت في مفهوم النص.

طعن المحكوم عليه على الحكم بطريق التميز، ونعى عليه بأن قد شابه القصور في التسبيب والفساد في الاستدلال والخطأ في تطبيق القانون؛ ذلك أنه لا جريمةَ ولا عقوبةَ إلا بنص، والمشرّع هو الذي يضع النصوص التجريمية، وقد اخطأ الحكم المطعون فيه إذ استند في ادانة الطاعن الى المادة 46/ 5 من القانون رقم 1/ 1991 في شأن مؤسسة الإمارات للاتصالات، إذ كيَّف الأعمال المسندة إلى الطاعن بأنها جنحة استخدام خدمة الإنترنت دون بيان السند القانوني في تجريم هذه الأعمال وعدم مشروعيتها. كما أن القانون المذكور لا يمكن تطبيقه على الواقعة المسندة إلى الطاعن لأنه لا يشتمل على أي نصوص أو مواد متعلقة بخدمة الإنترنت أو الجرائم التي تترتب على استخدامه، نظراً لأن هذا القانون قد صدر في تاريخ سابق على وجود نظام الإنترنت في الدولة وأخطأ الحكم في إدانة الطاعن عن التهمة الثانية إعمالاً للمادة 380 عقوبات، التي تعاقب على فض الرسائل والبرقيات دون إذن صاحبها والأعمال المسندة إلى الطاعن تخرج تماماً عن نطاق هذه المادة ولا يجوز القياس عليها، إذ هي تتعلق بالرسائل والبرقيات المكتوبة ولم يوضّح الحكم ما هي الطرق المصرح باستخدامها عند استخدام الإنترنت والطرق غير المصرح بها وسند ذلك في القانون. كما جاء بأسباب الحكم أن الطاعن دخل إلى المواقع المحظور دخولها دون أن يبين سند هذا الحظر والنص القانوني المستند إليه، وقد تخلف ركن القصد الجنائي لدى الطاعن إذ إنه لم يقم بالإطلاع على الرسائل البريدية الخاصة

بموظفي الهيئة عمداً بل اطلع على بعض الرسائل الموجودة في جهاز عام دخل إليه مصادفة بدلالة أقوال الشاهد مدير التشغيل بشبكة الإنترنت التي تفيد أن الطاعن لم يدخل على صندوق بريد خاص بأي من موظفي المؤسسة، وإنما دخل الجهاز الخاص بإرسال الرسائل البريدية وهو لا يشكل جريمة معاقب عليها، مما يعيب الحكم بما يستوجب نقضه.

5) **تأييد محكمة التمييز لإدانة المتهم وتبرير الحكم،** وقد جاء فى قضاء محكمة التمييز أن التهمتين تحقق ثبوتهما في حق الطاعن بأدلة سائغة لها معينها الصحيح من أوراق الدعوى، ومن شأنها أن تؤدي إلى ما رتّبه الحكم عليها مستمدة مما شهد به (الشهود) وتقرير المختبر الجنائي والمضبوطات، واعتراف المتهم بتحقيقات النيابة العامة... لما كان ذلك، ولئن كان الأصل أنه يجب التحرز في تفسير القوانين الجزائية والتزام جانب الدقة في ذلك وعدم تحميل عباراتها فوق ما تحتمل، إلا وأنه في حالة غموض النص فإن ذلك لا يحول دون تفسيره على هدي مما يستخلص من مقصد الشارع وما يحقق الغاية التي تغيَّاها من تقريره، كما أن لمحكمة الموضوع تكييف بعض الأمور غير المحددة في القانون على أن يكون هذا التكييف خاضعاً لرقابة محكمة التمييز. ومن المقرر أيضا أنه إذا ورد في النص التشريعي لفظ مطلق ولم يقم الدليل على تقييده، فقد أفاد ثبوت الحكم على إطلاقه ولما كانت المادة 46 من القانون رقم 1/ 1991 تنص على عقاب كل من يستخدم الأجهزة أو الخدمات أو التسهيلات التي تقدمها المؤسسة في الازعاج أو إيذاء مشاعر الآخرين أو أي غرض آخر غير مشروع. وكانت هذه العبارة قد وردت على سبيل الإطلاق في مجال بيان الأعمال المؤثّمة ما مفاده شمول الحظر لكل فعل غير مشروع في نطاق أعمالها أيا كانت طبيعته طالما خرج عن الغرض المحدد له في استخدام الشبكة طبقاً للنصوص المستخدم عليها في المادة 12 من القانون والمعاقب عليها في المادة 45 منه.. لما كان ذلك

وكان الحكم المطعون فيه، وفي حدود السلطة التقديرية، وفي التفسيير وفي التكييف، قد أورد في أسبابه ان الغرض غير المشروع على إطلاق عبارة النص يشمل كل فعل او امتناع عن فعل تجرّمه القوانين أو اللوائح، وأن ما قام به المتهم باعترافه من اختراقه شبكة الاتصالات (الإنترنت) التابعة لمؤسسة الإمارات، مستخدماً برامج للبحث عن الثغرات، واستطاع بذلك الحصول على كلمات السر لبعض المواقع المحظور على غير موظفي المؤسسة الدخول إليها، وقام بفك شفرة بعض الأجهزة ونسخ بعض الملفات وهو يعلم بحظر ذلك لغير موظفي المؤسسة المرخص لهم، كما قام بفكّ رسائل البريد الإلكتروني لبعض الموظفين ونقلها إلى جهاز الحاسب الآلي الخاص به مما يشكل استغلالاً للشبكة لغرض غير مشروع يوقعه تحت طائلة العقاب وهي أسباب سائغة تتفق وصحيح القانون وتتوافر فيها الأركان القانونية للتهمة الأولى المسندة إلى الطاعن كافة مما يكون معه معناه ـ في هذا الخصوص ـ غير سديد. . . . لمّا كان ذلك وكانت خدمة الإنترنت تدخل ضمن الخدمات التي تقدمها مؤسسة الاتصالات وتخضع لأحكام القانون رقم 1/ 1991 الخاص بمؤسسة الاتصالات، فإن ذلك لا يتعارض مع عدم صدور تشريع خاص بخدمات الإنترنت ويكون نفي الطاعن في هذا الصدد غير مقبول. . لما كان ذلك، وكانت المادة 380 عقوبات تعاقب على فض الرسائل و البرقيات بغير رِضاءِ من أُرسلت إليه وهو ما يسري على البرقيات سواءٌ كانت مكتوبة أو مرئية أو مسموعة، دون قصرها على المحررات المكتوبة حسبما يدعي الطاعن. وإذ دان الحكم المطعون فيه الطاعن لاستخدامه خدمة الإنترنت لهذا الغرض غير المشروع، وهو الاطلاع على الرسائل الخاصة دون رضاء أصحابها، فإنه يكون قد أصاب صحيح القانون ويكون نَفْي الطاعن في هذا الخصوص في غير محله. . . لما كان ما تقدم فإن الطعن برمته يكون على غير أساس متعين الرفض موضوعاً، وعليه حكمت المحكمة برفض الطعن.

وبالنظر الي عبارات محكمة التمييز فإننا نجد أنها أشارت إلى غموض النص، وأنه يجب التحرز في تفسير النصوص الجنائية وعدم تحميل عباراتها ما لا تحتمل، وأنها أدانت المتهم بالنظر إلي الغاية التي تغيّاها المشرع، وفسرت النص في ضوء تلك الغاية والمقصد المشروع.

وغنيٌ عن البيان أن عبارات محكمة التمييز في تبريرها للحكم توحي بأن هناك حاجة لإزالة الغموض وعدم ترك مسائل تجريم الأعمال المتصلة بالحاسب الآلي وشبكة الإنترنت للاجتهاد والقياس في تفسير النصوص للتمكن من إدانة المتهمين، وأولئك الذين ارتكبو أعمالاً قد تكون نتائجها وخيمة، لاتقدر بثمن، وتضر بمصالح شخصية، وقومية يحظر المساس بها، وأنه لابد من سن تشريعات صريحة ومتخصصة في مجال الجريمة الحديثة جريمة تقنية المعلومات.

**2 ـ عرضٌ لجريمة أخرى وقعت في دولة الإمارات العربية المتحدة بعد صدور قانون مكافحة جرائم تقنية المعلومات رقم 2/ 2006**

وقعت هذه الجريمة في شهر يونيو من عام 2006 بدبي وقدمت النيابة العامة اثنين من المتهمين فيها للمحاكمة ـ وهي أول جريمة تقدم استناداً لقانون مكافحة جرائم المعلومات الإماراتى ويُدان مرتكبها ـ واتهمت النيابة العامة بدبي المتهم الأول بأنه (توصل عن طريق الشبكة المعلوماتيه إلى الاستيلاء على مال منقول (عدد خمس تذاكر سفر) عائد لشركة سفريات وسياحة بدبي بطريقة إحتيالية وباتخاذ صفة غير صحيحة بأن تمكن من دخول موقع الشركة الإلكتروني عن طريق استخدام الرقم السري واسم المستخدم (الخاصّين بالمتهم الثاني) وهو أحد موظفي الشركة وكان ذلك من شأنه خداع الشركة وحملها على تسليم تذاكر السفر.

واتهمت النيابة الثاني بأنه اشترك بالاتفاق والمساعدة مع المتهم الأول بارتكاب الجريمة المبينة في الوصف السابق فوقعت الجريمة بناء على ذلك

الاتفاق والمساعدة، كما اتهمته بأنه بحكم عمله لدى الشركة بمهنة بائع تذاكر أفشى سرّ مهنته (الرقم السري واسم المستخدم) في غير الأحوال المصرّح بها قانوناً واستعمله لمصلحته الخاصة ومصلحة المتهم الأول دون إذن من صاحب الشأن.

وطلبت النيابة عقابهما بالمواد (1، 10، 23، 25) من القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات والمادة 379 من قانون العقوبات الاتحادي.

وقد دافع المتهم الأول عن التهمة الموجهة له بأنه لم يكن يقصد الاحتيال، وقد ردت المحكمة هذا الدفاع بأن المتهم قد اتفق مع المتهم الثاني (الموظف بالشركة الهارب) وحصل منه على الرقم السري واسم المستخدم الخاصّين به، وقام في أزمنة مختلفة باستخدامها عن طريق الدخول على موقع الشركة وتمكن من الحصول على التذاكر باعترافه، مع أنه ليس له صفة الدخول ولايحق له استخدام الرقم السري واسم المستخدم، مما يشكل فعله طريقة احتياليه باتخاذ صفة غير صحيحة ليتمكن من الدخول للموقع وكان من شأن ذلك خداع الشركة وحملها على تسليم تذاكر السفر المبينة بالأوراق.

وقد أدانتهما المحكمة طبقاً للمادة 212 من قانون الإجراءات الجزائية الإماراتى والمواد (1، 10، 23، 25) من قانون جرائم تقنية المعلومات والمادة 379 من قانون العقوبات وحكمت على المتهم الأول بالحبس لمدة شهرين وإبعاده عن البلاد، وعلى المتهم الثاني بالحبس لمدة سنة واحدة وإبعاده عن البلاد.

وقد أعملت المحكمة قواعد الارتباط المقررة في القانون بالنسبة للتهم الموجهه للمتهم الثاني وعاقبته بالعقوبة المقررة للجريمة الأشدّ، كما أنها طبقت أحكام المواد 99 و100 من قانون العقوبات وعاملت المتهم الأول بقسط من الرأفة لظروف الدعوى وتنازل المجني عليها (الشركة).

# الفصل الرابع
# الجرائم الرقمية والإلكترونية في الغرب وآليات مواجهتها

يتناول هذا الفصل الجريمة الإلكترونية فى أوروبا وأمريكا عبر أربعة مباحث، انفرد المبحث الأول بالحديث عن تطور حجم خسائر الجرائم المعلوماتية فى الدول الغربية، أما المبحث الثاني فقد اختص بتناول الجريمة الإلكترونية بين التشريع والقضاء فى الدول الغربية فيما ركز المبحث الثالث على موقف التشريعات اللاتينية من جريمة سرقة المعلومات، وأخيراً جاء المبحث الرابع متحدثاً عن آليات مكافحة الجريمة الإلكترونية فى الدول الغربية.

## المبحث الأول:
## الخسائر التي خلّفتها الجرائم الرقمية فى الغرب

يصعب تقدير حجم الخسائر المترتبة على جرائم نظم المعلومات[1]

---

(1) المخربون : يقوم المخربون باستخدام بعض الوسائل الأوتوماتيكية لاكتشاف نقاط الضعف في نظم الكمبيوتر بغرض زرع البرنامج المدمر في تلك النظم، ويظل هذا البرنامج كامناً حتى يحين موعد الهجوم المحدد. فإذا ما قام المخربون بزرع البرنامج المذكور عبر جهاز كمبيوتر خاص بشخص آخر فإن ذلك يزيد من صعوبة تعقبهم.

راجع في ذلك: Dr: Linda Volonino. Cybet Terrorism. Op. cit.

والسبب في ذلك الرقم الأسود الذي يسيطر على هذا النوع من الإجرام، علاوة على الموقف السلبي للمجني عليهم في هذه الجرائم، ولصعوبة اكتشاف الجريمة المعلوماتية[1].

لذا فإنه من الصعوبة تقدير حجم الخسائر الناشئة عن هذه الجرائم[2] كما تشير بذلك الأبحاث التي أجريت في هذا الشأن سواء في فرنسا أو الولايات المتحدة الأمريكية أو إنجلترا.

## تقدير خسائر الجرائم المعلوماتية في الولايات المتحدة الأمريكية

أجرى المكتب الأعلى للإحصاء la general Accounting office عام 1976 تحقيقاً بخصوص ظاهرة الغش في الأنظمة المعلوماتية الخاصة بالحكومة الفيدرالية، وجاءت نتيجته على النحو التالي :

- 40٪ حالات اختلاس أشياء مختزنة ترتب عليها خسارة قدرت بحوالى 57,000 دولار.
- 39٪ حالات اختلاس أموال تسببت في خسارة قدرت بـ 34,000 دولار.
- 12٪ حالات تعديل غير مسموح به في البيانات.

---

(1) Bertin et Lambertie, la protection du logiciel, enjeux juridiques et economiques L.G.D.J.1985, p. 30

(2) وتجدر الإشارة في هذا الصدد إلى أن إحجام ضحايا الجرائم المعلوماتية عن الإبلاغ عن الجرائم المرتكبة في حقهم ـ سواء لخوفهم من الفضيحة أو لاعتقادهم بعدم قدرة الشرطة على التعامل مع مثل هذه الجرائم، أو لعدم درايتهم من حيث المبدأ ـ لوقوع مثل هذه الجرائم ـ أن هذا الإحجام يؤدي إلى فرار المجرمين من العقاب كما أنه يترك وحدات جرائم الكمبيوتر الشرطية التي تتمتع بكفاءة عالية دون عمل يذكر، ومن هنا يظل النطاق الحقيقي لجرائم الكمبيوتر : حجمها، طبيعتها ومداها وتهديداتها ـ تظل كلها أمور غامضة، انظر :
HACKER CRACK DOWN Law and Disorder on the Electronic Frontier b: Bruce sterling p. 168. 1994.

- 6٪ حالات استخدام غير مسموح به للأنظمة المعلوماتية.
- 3٪ حالات إتلاف.

وغالبية أفعال الغش ارتكبت عن طريق إدخال بيانات مصطنعة 62٪. ثم يلي ذلك الاستعمال غير المشروع للوسائل المعلوماتية «25٪» ويأتي في المرتبة الثالثة تعديل المعالجات المعلوماتية «23٪» وأخيراً اختلاس الوثائق الصادرة عن الحساب الآلي «17٪»[1].

وأجريت دراسة عام 1984، بواسطة المعهد الأمريكي للتصديق على الإحصاء العام بخصوص الغش المعلوماتي في البنوك وشركات التأمين، والتي انتهت إلى أنه في غالبية الحالات «60٪» يتحقق الغش عن طريق التلاعب في الصفقات، إما بخلق معلومات مصطنعة أو إتلاف أو تعديل بيانات حقيقية، وفي ثلث الحالات عن طريق التعديل في مناطق تسجيل الملفات، وإن استمرار فعل الغش يرتبط بالوضع الوظيفي لمرتكبه. وهكذا فإن 41٪ من حالات الغش بوشرت عن طريق مستخدمين استمرت لمدة أقل من سنة واحدة، 15٪ من تلك الحالات نفذت بوساطة مسؤولين استمرت لمدة أكثر من سنة، ويتوافر لهذه الفئة الأخيرة إمكانيات لإخفاء أفعالهم، ويتطابق الوضع الوظيفي والمبالغ المتحصلة من أفعال الغش حيث أن 59٪ من حالات الغش والتي قدرت بأقل من 25,000 دولار قد تم ارتكابها بواسطة مستخدمين في البنوك و85٪ في شركات التأمين، بينما نسبت أفعال الغش التي تجاوزت 1000,000 دولار إلى المستخدمين الذين يشغلون مراكز متقدمة[2].

وباشر الاتحاد الأمريكي للمحامين تحقيقاً عام 1984 على 283 منشأة ومؤسسة كبرى، وتبين أن ثلثيهما وقعتا ضحية لظاهرة الغش في المعلومات

(1) انظر د. محمد سامي الشوا، ـ ثورة المعلومات وانعكاساتها على قانون العقوبات، ص 25.
(2) المرجع السابق.

بدرجات متفاوتة. كما أظهر التحقيق، أنه عندما يكون الحاسب الآلي موضوعاً للجريمة، فإن ثماني منشآت من عشر تعتبر أن محو أو إتلاف البيانات يمثل النمط الأكثر خطورة لهذه الظاهرة، والأمر نفسه بالنسبة لسرقة أو إتلاف البرامج، وعلى النقيض بالنسبة لسرقة أو إتلاف المعدات المادية، فهي تبدو، على وجه التحديد اقل خطورة.

ويستحيل نسبياً معرفة إجمالي الخسائر التي لحقت بالمنشآت الأمريكية ووفقاً لتقدير الاتحاد الأمريكي للمحامين، فإن ربع هذه المنشآت قد عانت من خسائر في العام السابق على إجراء التحقيق، تفاوتت من 145 إلى 730 مليون دولار، وهذا يعكس تبايناً واضحاً في الخسارة من منشأة إلى أخرى. وعلى وجه العموم فقد قدرت بأقل 100,000 دولار بالنسبة لـ 20٪ من هذه المنشآت. وقدرت بأكثر من مليون دولار لـ 4٪ منها، وأن 28٪ من هذه المنشآت لم تعلم مقدار الخسارة التي لحقت بها من أثر الغش المعلوماتي[1].

## تقدير حجم خسائر الجرائم المعلوماتية في إنجلترا

قدر اتحاد الصناعات الإنجليزية عام 1976 الخسائر الناشئة عن الغش المعلوماتي بمبلغ يتراوح ما بين 25 إلى 30 مليون جنيه استرليني في السنة.

وتوضح الدراسة التي قام بها K.Wong على 95 حالة غش معلوماتي، أن متوسط الخسارة فيها بلغ 30,000 جنيه إسترليني. كما أبانت عن أن سرقة المعدات المادية ولاسيما «الحاسبات الآلية الميكروية» والحرائق العمدية والإتلاف، لا تمثل كل منها سوى 30٪ من الحالات محل الدراسة. ومع ذلك فإن خسائرها كانت مرتفعة جداً.

وبالنسبة لسرقة المعلومات والبرامج «وتمثل 15٪ من الحالات»، فهي

---

(1) المرجع السابق.

تباشر بصفة أساسية عندما يحل المستخدمون محل الأجراء، وأن إتلاف التجهيزات غالباً ما يتسبب به الطاقم المسؤول عن تشغيل وتخزين الدعائم الممغنطة، ولكن بالنسبة لإتلاف وظيفة النظام bombes logiques «8٪» فهو من صنع المبرمجين أو أصحاب البرامج. ويمثل انتهاك الأنظمة المعلوماتية بغرض الحصول على معلومات أو خدمات مجانية نسبةً تقدر بحوالى العُشْر، ولكن هذا النمط من الإجرام سيتضاعف بسبب انتشار الحاسبات الميكروية المنزلية[1].

## تقدير خسائر الجرائم المعلوماتية في فرنسا

ارتفع معدل الخسائر الناتجة عن المعلوماتية في فرنسا حيث بلغت عام 1986 وفقاً لإحصاء الجمعية العمومية لشركات التأمين ضد الحرائق والمخاطر المختلفة APSAIRO حوالى 7,3 مليار فرنك فرنسي، ويرجع 46٪ منها إلى الأفعال الإجرامية و 30٪ إلى المخاطر العارضة و24٪ إلى الأخطاء.

ويتبين من تحليل الخسائر المرتبطة بجرائم المعلومات في فرنسا أن 60٪ منها يتعلق بالبرامج، ويتركز الغش في معظم هذه الحالات في اتفاقات غير مشروعة (35٪) واستغلال الأعطال القائمة 10٪ وتضليل البرامج 9٪، ومن ناحية التشغيل فإن 25٪ من الخسائر ترجع إلى تعديل الإجراءات والملفات والسهو المتعمَّد ونقل البيانات.

وقد تضاعفت خسائر سرقة البرامج المنطقية ذوات النمط الواحد في الفترة ما بين 1984 إلى 1985 وفقاً لتقدير وكالة حماية البرامج لتصل إلى 1,12 مليار فرنك ويرجع 43٪ من هذه الخسائر إلى سرقة أدوات البرامج المنطقية ذوات النمط الواحد «كبرامج الفائدة الخاصة بالتصنيف والمعاونة في تصميم برامج وإدارات البيانات والأمن وصيانة البرامج، و30٪ للبرامج المنطقية التطبيقية ذوات

(1) المرجع السابق ص ص 27 – 28.

النمط الواحد الخاصة بالسداد والمحاسبة وإدارة الوثائق، 17٪ للبرامج المنطقية الأساسية ذوات النمط الواحد الخاصة بأنظمة التشغيل، وقدرت خسائر الألعاب بحوالى 10٪. ويشهد معدل الخسائر في مجال صفقات الإنتاج وشركات الخدمات والمنشآت الناشرة للبرامج ارتفاعاً ملحوظاً حيث وصلت الخسائر إلى 19٪ في عام 1985، 50٪ منها للحاسب الآلي الميكروي، و11٪ للأنظمة المتوسطة والكبيرة[1].

## المجالات المستهدفة في مجال جرائم سرقة نظم المعلومات

يتركز الاتجاه الأساسي لجرائم نظم المعلومات وفقاً لتحقيق أجرته مجلة Ressources informatiqes في أنّ :

19 ٪ من أفعال الغش المعلوماتي تستهدف البنوك.

16٪ الإدارة.

10٪ الإنتاج الصناعي.

10٪ المعلومات.

ثم يلي ذلك شركات التأمين والشركات الخاصة. وفي واقع الأمر إن جرائم نظم المعلومات تستهدف في المقام الأول المؤسسات المالية والتي تتحكم في القيم الرأسمالية.

ويمكن التأكيد، من جهة أخرى، على أن المعلومات قد صارت أحد المصالح الأساسية المستهدفة بعد النفوذ حيث أصبحت هي المنفذ إلى اقتصاد السوق وقد بني على أساسها بصناعة المعلومات.

وقد نما إلى جوار «السوق الشرعي للمعلومات» marche legalde

(1) انظر في ذلك المرجع السابق ص ص 20 ـ 21.

information السوق السوداء للمعلومات وفيه تتم مقايضة وبيع المعلومات المسروقة أو المقتبسة من أصحابها الحقيقيين والشرعيين، ويرتبط هذا النوع من الإجرام إذن بالجزء الأعظم للأنشطة الاقتصادية والاجتماعية للمجتمع. ويمكن تصوره بالنسبة للمعلومات الآتية :

**أ ـ المعلومات المالية :**

حيث تمسّ هذه الظاهرة المركز الحسابي والإداري وتنقلات الأموال والاستثمارات سواء في المنشآت العامة أو الخاصة.

**ب ـ المعلومات التجارية والصناعية :**

حيث تستهدف هذه الظاهرة الدراسات الخاصة بالأسواق ومشروعات الاستثمار والتصنيع والإنتاج والتجارة والتوزيع والأسعار ومراكز البيع والقطاع الصناعي للإنتاج.

**جـ ـ المعلومات الشخصية :**

وهي تلك المختزنة في ذاكرات الحاسبات الآلية للبنوك وشركات التأمين ولدى المحامين والمستشفيات وأقسام الشرطة والأحزاب والنقابات. وقد تهدد هذه الاعتداءات مباشرة قدسية وسرية الحياة الخاصة أو الحرية النقابية والسياسية. . . إلخ.

**د ـ المعلومات العسكرية :**

والتي تتمثل في أسرار الدولة والمشروعات النووية والتصنيع الحديث للأسلحة. . . إلخ.

ويبدو أن هذه المعلومات الأخيرة هي الأكثر رواجاً في «سوق المعلومات السوداء».

ويمكن الاستئثار بهذه المعلومات عن طريق معالجتها معالجة معلوماتية

farun traitement in formatique ومؤدّى ذلك أن مجرد المعالجة المعلوماتية يسمح بإدارتها على نحو جيد وعلى الرغم من المخاطر التي يمكن أن تتعرض لها هذه الإدارة الآلية.

وتجدر الإشارة إلى أن هذه المعلومات من خلال تداولها واستخدامها عبر الحاسب الآلي أصبحت عرضة للتلف والدمار، وتالياً، لا يستطيع المشتري الاستفادة منها سواء كان ذلك بسبب يرجع إلى البائع أو الغير، من خلال ما يعرف بفيروس الحاسب الآلي. وفي ظل التطور الهائل المحسوس في عصرنا الحالي من اتساع درجة الاعتماد على استخدام المعلومات المبرمجة من خلال الحاسبات الآلية وما قد ينشأ عن ذلك من أضرار قد تلحق بالمعلومات نفسها إذا ما أصابها التلف والضرر من جراء فيروسات الحاسبات الآلية أو الضرر الذي يلحق بمستخدميها، فهنا بالتأكيد ستقوم المسؤولية تجاه الشخص الذي تسبب في هذا الضرر ويجب عليه التعويض عما لحق بالآخرين من ضرر.

## المبحث الثاني:
## الجرائم الرقمية والإلكترونية
## في التشريع والقضاء الغربيين

تعتبر السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والإنترنت، حيث صدر قانون البيانات السويدي عام (1973م) الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشروع عليها.

وتبعت الولايات المتحدة الأمريكية السويد حيث شرّعت قانوناً خاصاً بحماية أنظمة الحاسب الآلي (1976م ـ 1985م)، وفي عام (1985م) حدّد معهد العدالة القومي خمسة أنواع رئيسة للجرائم المعلوماتية وهي: جرائم الحاسب

الآلي الداخلية، جرائم الاستخدام غير المشروع عن بعد، جرائم التلاعب بالحاسب الآلي، دعم التعاملات الإجرامية، وسرقة البرامج الجاهزة والمكونات المادية للحاسب. وفي عام (1986م) صدر قانون تشريع يحمل الرقم (1213) عرّف فيه جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية كما وضعت المتطلبات الدستورية اللازمة لتطبيقه، وعلى اثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي.

وتأتي بريطانيا كثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي حيث أقرت قانون مكافحة التزوير والتزييف عام (1981م) الذي شمل في تعاريفه الخاصة تعريف أداة التزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو بأية طريقة أخرى.

وتطبق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلي والإنترنت حيث عدّلت في عام (1985م) قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والإنترنت، كما شمل القانون الجديد تحديد عقوبات المخالفات الحاسوبية، وجرائم التدمير، أو الدخول غير المشروع لأنظمة الحاسب الآلي.

وفي عام (1985م) سنّت الدنمارك أول قوانينها الخاصة بجرائم الحاسب الآلي والإنترنت والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروع إلى الحاسب الآلي أو التزوير أو أي كسب غير مشروع، سواءٌ للجاني أو لطرف ثالث أو التلاعب غير المشروع ببيانات الحاسب الآلي كإتلافها أو تغييرها أو الاستفادة منها.

وكانت فرنسا من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت في عام (1988م) القانون رقم (19 ـ 88)

الذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها.

أما في هولندا فلقاضي التحقيق الحق بإصدار أمره بالتنصت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة، كما يجيز القانون الفنلندي لمأمور الضبط القضائي حق التنصت على المكالمات الخاصة بشبكات الحاسب الآلي، كذلك تعطي القوانين الألمانية الحق للقاضي بإصدار أمره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها وذلك خلال مدة أقصاها ثلاثة أيام.

كما يوجد في المجر وبولندا قوانين خاصة بجرائم الحاسب الآلي والإنترنت توضح كيفية التعامل مع تلك الجرائم ومع المتهمين فيها، وتعطي تلك القوانين المتهم الحق في عدم طبع سجلات الحاسب الآلي أو إفشاء كلمات السر أو الأكواد الخاصة بالبرامج.

وغير ذلك من الدول الأوروبية هولندا والمجر وبولندا...كل الدول عدلت من القوانين الجنائية ليتم إدخال الجرائم المعلوماتيه فى إطار قانونى ويتمّ تجريم كل ما يشملها من عمليات احتيال ونصب وملكيه فكرية واختراق أجهزة الآخرين وما إلى ذلك. ولكن مع الأسف على المستوى العربي لم تقم دولة عربية بسن قوانين خاصة بالحاسب الآلي والإنترنت، وكذا الحال بالنسبة لمملكة البحرين فلا توجد قوانين خاصة بجرائم الإنترنت، وان وجد نص قريب من الفعل المرتكب فان العقوبة المنصوص عليها لا تتلاءم وحجم الأضرار المترتبة على جريمة الإنترنت.

## نماذج لجرائم معلوماتية ارتكبت فى الدول الغربية

1 - في بنك لويدز في أمستردام، قام شاب عمره 26 سنة بتحويل مبلغ 8,4 مليون دولار عبر نظام الحوالات العالمية من فرع هذا البنك في نيويورك

إلى حساب في بنك آخر في سويسرا. واعتقلت الشرطة في إحدى مدن ولاية أوريجن الأمريكية شابًا عاطلاً عن العمل عمره 26 عامًا استخدم أحد مواقع الدردشة على الإنترنت لتنظيم انتحار جماعي فيما يسمى بعيد الحب هذا العام لمن لم يوفق في حياته العاطفية.

2 ـ روبر مورس شاب أمريكي يبلغ من العمر 23 عامًا أطلق فيروسًا باسمه دمّر ستة آلاف نظام عبر الإنترنت بينها أجهزة عدد من المؤسسات الحكومية بخسائر بلغت مئة مليون دولار، عوقب على إثرها بالسجن لمدة 3 سنوات.

3 ـ أما تيموثي ألن ليود (35 عامًا) فهو مصمم ومبرمج فُصل من عمله، فما كان منه إلا أن أطلق قنبلة إلكترونية ألغت جميع التصاميم وبرامج الإنتاج لأحد أكبر مصانع التقنية العالية في نيوجرسي التي تعمل لحساب وكالة الفضاء NASA والبحرية الأمريكية.

4 ـ الشاب الفرنسي جان كلود، خلافاً لسلوك العصابات، فرغم أنه استطاع تصميم بطاقة صرف آلي وسحب بها مبالغ من أحد البنوك، إلا أنه ذهب إلى البنك وأعاد إليه المبالغ وأخبرهم أنه فعل ذلك ليؤكد لهم أن نظام الحماية في بطاقات الصرف الخاصة بالبنك ضعيف ويمكن اختراقه، إلا أن ذلك لم يمنع الشرطة الفرنسية من إلقاء القبض عليه ومحاكمته. الأمر نفسه فعلته مجموعة من الشباب الأمريكي أطلقوا على أنفسهم «الجحيم العالمي» إذ تمكنوا من اختراق مواقع البيت الأبيض، والمباحث الفيدرالية، والجيش، ووزارة الداخلية؛ لكنهم لم يخربوا تلك المواقع، بل اقتصر دورهم على إثبات ضعف نظام الحماية في تلك المواقع، إلا أنهم حوكموا أيضًا. وقبل 5 سنوات ألقت السلطات الإسرائيلية القبض على شابين شقيقين ضريرين من الفلسطينيين ووجهت إليهما تهمة اختراق مواقع وزارة الدفاع الإسرائيلية.

وفي واقع الأمر إن لغة الأرقام تؤكد أننا أمام تحدٍّ خطير، فخسائر الشركات الصناعية والتجارية في بريطانيا من جرائم الإنترنت تجاوزت 1,1 مليار جنيه استرليني. أما مكتب التحقيقات الفيدرالية الأمريكية (FBI) فقدر حجم الخسائر الناجمة عن الجرائم الإلكترونية في أمريكا بحوالى 10 مليارات دولار سنويًا عام 1998م، ارتفعت إلى 14 مليار عام 2004م.

والمثير أن 17٪ فقط من الضحايا يبلِّغون عن هذه الجرائم التي يصل معدلها إلى ألف جريمة يوميًا. معهد أمن المعلومات أجرى دراسة مسحية بالتعاون مع مكتب التحقيقات الفيدرالية على 538 مؤسسة وشركة أمريكية فتبين أن 85٪ منها تعرضت لاختراقات إلكترونية، 70٪ منها جاءت عبر الإنترنت، و65٪ منها ألحقت خسائر مادية بالمؤسسة. ولم يتمكن سوى 35٪ من الشركات من حصر هذه الخسائر. لم يكن غريبًا والأمر كذلك أن يطلب الرئيس الأمريكي السابق بيل كلنتون في يناير عام 2000م من الكونجرس تخصيص 2 مليار دولار لمكافحة جرائم الإنترنت.

5 ـ قدمت الولايات المتحدة الأمريكية، مواطناً أمريكياً للمحاكمة الجنائية نتيجة قيامه بتقديم خدمة المقامرة عن طريق الانترنت، وإنشاء هذا الموقع في دولة انتيغوا وبربودا، وبيعه هذه الخدمة لمواطني الولايات المتحدة الأمريكية، بالمخالفة لقانون الاتصالات السلكية لسنة 1961 (Wire Communication Act of 1961)، وهنا قضت المحكمة بحبسه 21 شهراً، ومنعت الموقع من الاستمرار. وبما أن اتفاقية «الجاتس» تنظم تبادل الخدمات عبر الحدود، وأمريكا ودولتا انتيغوا وبربودا عضوان في الاتفاقية، فقد قدمت الأخيرة شكوى إلى لجنة فض المنازعات معتبرة حكم المحكمة الأمريكية مخالفاً للاتفاقية وعائقاً لحركة التجارة عبر الحدود.

ادعت أمريكا انها تمنع المقامرة عبر الإنترنت في ولاياتها وفقاً لقوانينها،

وأن المقامرة عبر الإنترنت تشكل مخالفة للآداب العامة، وأن المنع كان ضرورياً ومبرراً لحماية الأحداث من الوقوع في براثن المقامرين، ومنعاً للجريمة المنظمة وغسيل الأموال، ومن ثمّ فإن لها الحق في منع مثل هذه الخدمات الإلكترونية والتي تقدمها دولة انتيغوا وبربودا، وأن ذلك الحظر، أو المنع، جاء متفقاً مع اتفاقية الجاتس في المادة السابعة عشرة فقرة (أ) والتي تمنح الدول الحق في وضع قيود على الخدمات التي تخالف الآداب العامة والنظام العام.

في 11 نوفمبر 2004 أصدرت اللجنة قرارها بأنّ الحظر والمنع الكامل للمقامرة عبر الإنترنت والتي تقدم من دولة انتيغوا وبربودا لمواطني الولايات المتحدة الأمريكية، غير مبَّرر وأن أمريكا تعسفت في استعمال حقها، لذلك فإن على أمريكا أن تلغي هذا المنع والحظر وفقا للاتفاقية ولتسهيل حركة التجارة والخدمات عبر الحدود.

وقد استندت لجنة فض المنازعات فى رفضها للأعذار المقدمة من أمريكا بناء على سببين رئيسين :

(1) على الرغم من الحظر المفروض بسبب الآداب أو الأخلاق العامة، كان ينبغي على أمريكا التفاوض مع انتيغوا وبربودا لمعرفة ما إذا كانت هناك بدائل أخرى أقل تقييداً لحرية التجارة بدلاً من المنع الكامل، وعلى هذا الأساس فإن اللجنة لم تجد أن الحظر كان ضرورياً لحماية الآداب العامة كما هو مطلوب في المادة السابعة عشرة.

(2) وجدت اللجنة أن أمريكا كانت تتعامل بطريقة فيها تمييز لصالح المورّدين الأمريكيين، وأن تطبيقها للقانون كان غير محايد، حيث كانت تتم محاكمة الموردين الأجانب أكثر من الموردين الأمريكيين مما يعطي انطباعاً أن أمريكا تفضل الموّردين المحليين على الموّردين الأجانب بدلاً من تطبيق القانون المحلي الأمريكي على الجميع بدون محاباة أو تمييز.

هذه القضية تعتبر مهمة لسببين رئيسين: أولاً: أنها متعلقة بالمقامرة عن

طريق الإنترنت وما إذا كانت المقامرة تشكل مخالفة للآداب العامة من عدمه، أو أن هناك وسائل وطرقاً أخرى للتقليل من آثاره بدلاً من المنع الكامل أو أنّ المنع كان ضرورياً لحماية الأخلاق العامة.

ثانياً: اتضح دور منظمة التجارة العالمية في الإشراف على حركة التجارة والوصول إلى القوانين المحلية للنظر في مدى ملاءمتها واتفاقها مع اتفاقيات التجارة الدولية، وتفسيرها للنصوص وسلطتها التقديرية في تقدير الحماية الضرورية لحفظ الأخلاق العامة في كل دولة.

لذلك، وبسبب عدم وضوح المقصود بالآداب العامة في قانون العقوبات الاتحادي، وفي قانون جرائم تقنية المعلومات، وما هو الممنوع وما هو المباح، وما يشكل جريمة، فإن منظمة التجارة العالمية قد تلعب دوراً في التحديد وفي الإباحة قد لا يتفق مع غرض المشرّع ورأي المحكمة الاتحادية العليا، خصوصاً أن هناك أفعالاً قد تختلف فيها وجهة النظر، وأن السلطة العامة لم تتخذ فيها أي إجراء عقابي يدل على المنع، مما قد يوهم في ذهن المنظمة ولجنة فض المنازعات إلى أن الأمر مباح غير مُجرّم، وأن منع دخول سلعة أو وقفها أو منع الحصول عليها ككتاب الكتروني فيه تقييد لحركة التجارة بالمخالفة لاتفاقيات التجارة الدولية، مما يؤثر على الثقافة المحلية والعادات والتقاليد، ويجبر الطرف الآخر على قبول سلعة ما تخل بالآداب العامة وفقاً لمفهومها في القوانين المحلية.

إنّ الجرائم السابقة ذات الطابع الاقتصادي أو السياسي تلقى اهتمامًا واسعًا من المؤسسات المعنية بمكافحة جرائم الإنترنت، وهو اهتمام يفوق بمراحل الجرائم الأخلاقية على الإنترنت التي غدت من أكبر مسوّقي تجارة الجنس في العالم. ومن سوء الحظ أن مكافحة الجرائم الجنسية على الإنترنت كثيرًا ما تصطدم بعوائق تشريعية، ففى الولايات المتحدة الأمريكية، عطلت المحكمة العليا تطبيق قانون كان يستهدف حماية الأطفال من المواد الإباحية على الإنترنت رغم تزايد حالات استدراج الأطفال من خلال الشبكة والاعتداء الجنسي عليهم؛ القانون كان يفرض غرامة قدرها 5 ألف دولار على من ينشر مواد مؤذية للقُصّر

على صفحات الإنترنت ويجعل تلك المواد في متناولهم بشكل يسير، لكن المحكمة اعتبرته مقيدًا لضمانات حرية التعبير. الأمر نفسه حدث في هونج كونج، حيث فشلت سلطات التشريع في وضع حد لترويج مواد إباحية للأطفال على شبكة الإنترنت ورفضت مشروع قانون يقضي بالحبس على كل من يثبت امتلاكه مواد إباحية تتعلق بالأطفال، وقال المشرعون: إنهم يخشون أن تتخذ السلطات ذلك القانون ذريعة لمزيد من إحكام قبضتها على الإنترنت. وعلى العكس من أمريكا وهونج كونج، نجح المركز الأسترالي لمكافحة جرائم الإنترنت في توقيف وتفتيش 40 متهمًا بجرائم الاغتصاب والاستغلال الجنسي وتنظيم السياحة الجنسية وتوزيع أفلام دعارة باستخدام شبكة الإنترنت.

## وقائع قرصنة أمام القضاء الأمريكى

(1) ومن جرائم السرقة التي عرضت على القضاء الأمريكي، نذكر أن أخصائيّ كمبيوتر روسي الجنسية ومقيم فى مدينة a st.peters burg ويدعى Vladimir Levin هاجم نظم الكمبيوتر الخاص بـ city bank وذلك عبر واسطة asprint connection التي تربط روسيا بالولايات المتحدة ونجح فى الاستيلاء على مبلغ وقدره 10,000,000 عشرة ملايين دولار أمريكى من حسابات البنك وقد تم ضبط Levin فى لندن عام 1995 وحكمت عليه إحدى المحاكم الأمريكية عام 1997 بالسجن لمدة ثلاثة أعوام.

وتشير حادثة سرقة city bank والتى وقعت خلال الهجوم على نظام الكمبيوتر الخاص بهذا البنك، إلى تعاظم القدرات الإجرامية الخاصة بعصابات الجريمة المنظمة الروسية. ويشير التقرير الصادر بشأن الجريمة المنظمة الروسية[1] إلى أن وزارة الداخلية الروسية (m.v.o) قد نجحت أخيراً في حل لغز

(1) تقدر وزارة الداخلية الروسية وهى الوكالة الروسية المسؤولة عن مكافحة عصابة الجريمة المنظمة الروسية أن ما بين 50٪ إلى 85٪ من البنوك الروسية تخضع لسيطرة تلك العصابات.

إحدى جرائم الكمبيوتر الكبرى وذلك بالتعاون مع وحدة الخدمات الخاصة ببريطانيا وهولندا.

وتجدر الاشارة هنا إلى أن مجموعة كبيرة من موظفى البنوك الأجنبية قد زارت مقر city bank فى وقت سابق لوقوع الحادث بغرض دراسة نظام حماية الكمبيوتر الخاص بالبنك بصورة تفصيلية حتى يتمكنوا من تشغيل هذا النظام فى فروع البنك المنتشرة فى 96 دولة ومن بينها روسيا. ويعتقد أن المجرم قد اقتحم النظام من خلال وحدة الحماية الإلكترونية ثم قام بسحب كميات كبيرة من المال من حسابات مجموعة كبيرة ومختلفة من العملاء وقام بتحويلها إلى حسابات تخص شركائه فى الجريمة تم فتحها مسبقاً في بنوك مختلفة خارج البلاد.

**(2) عملية sundevil** [1]:

حظيت عملية sundevil بشعبية واسعة فاقت مثيلاتها من مختلف أنشطة مكافحة مخربى الكمبيوتر التي جرت عام 1990، فقد كانت حملة الضبطيات الواسعة التي استهدفت أجهزة الكمبيوتر المشتبه فيها فى سائر أرجاء الدولة والتى تمت فى 8 مايو 1990، حملة غير مسبوقة من حيث النطاق والتغطية الإعلامية.

لقد كانت عملية sundevil إجراءاً صارماً استهدف فرض النظام على أولئك المخربين التقليديين الذين يعيشون فى «ظلال العالم الرقمي» سارقي بطاقات الائتمان ومسيئي استخدام أكواد التليفون،وكانت مجموعة sundevil إحدى مجموعات مخربي الكمبيوتر والتى سميت العملية باسمها وهى أكبر المجموعات التي استهدفتها الحملة وأكثرها تنظيماً. وقد استهدفت عملية sundevil بوصفها حملة على الاحتيال الإلكتروني مجموعة منتقاة من جماعات

---

(1) أنظر فى ذلك :

The hacker Crackdown law and Disorder on the Electronic fron- tier by Bruce sterling p.159.1994.

المخربين تم اختيارها بعناية فائقة نتاجاً لتحريات وتحقيقات مفصّلة استمرت على مدار عامين كاملين.

ومرةً أخرى كانت الأهداف هى نظم «لوحات النشر»، وما من شك أن لوحات النشر قد تعد سنداً قوياً لعمليات الاحتيال المنظمة ودائماً ما تحوي لوحات النشر السرية الخاصة بالمخربين ـ والمتداولة بينهم ـ مناقشات حية ومفصلة ومكثفة وصارخة لجميع أساليب وأنشطة انتهاك القانون والإخلال به، وعلى الرغم من أن مناقشة تفصيلات القضايا الإجرامية ليست بالأمر غير المشروع، إلا أنه ليس بالإمكان أن نعتبر الأشخاص الذين يتآمرون للانحلال بالقانون مجرد أندية أو صالونات فكر أو جماعات مستخدمين أو دُعاة حرية رأي بل عادة ما توصّفهم الشرطة وأجهزة الادعاء «بالعصابات أو المنظمات الفاسدة أو عصابة الجريمة المنظمة».

وما هو أكثر من ذلك، أن المعلومات والبيانات غير المشروعة التي تحويها لوحات النشر ـ الخارجة عن القانون ـ تتخطى فى عمقها مرحلة الحديث أو التآمر الجنائي المجرد، فقد شهد حيز الممارسة فى ذلك العالم الرقمي السري عمليات نشر الآلاف من أكواد التليفونات على لوحات النشر الخاصة بالمخربين تركت مشاعاً لكل من تسول له نفسه إساءة استخدامها.

وقد حملت لوحات النشر الخفية المذكورة كذلك العديد من البرامج سهلة الاستخدام، التي تقوم باستعراض ومسح أكواد التليفونات وكذا المستخدمة فى الإغارة على نظم شركات بطاقات الائتمان، وفضلاً عن ذلك فلطالما شهدت لوحات النشر المذكورة العديد من البرامج التي تعرضت لعمليات القرصنة وكلمات السر التي تعرضت للانتهاك ومخططات الاقتحام وأدلة العمل لراغب الاختراق وملفات التخريب والملفات الفاضحة وغيرها.

وتحظى لوحات النشر بجانب حيوى شيق يثير اهتمام المحقق المحترف ألا وهو أنها تعج بالأدلة الهامة، فدائماً ما نجد أن لوحات النشر توثق عمليات

الاتجار فى البريد الالكتروني، كما تضم جميع الوقائع التي يتبجح المخترقون بنشرها تباهياً بأفعالهم غير المشروعة، كما تعتبر أكواد التليفون وأرقام بطاقات الائتمان المسروقة ذاتها توثيقاً إلكترونياً وحقيقياً لأوجه النشاط الاجرامي. ويجب على المحقق- حال ضبطه لإحدى لوحات النشر الخاصة بالقراصنة أن يتعامل مع هذا الدليل بالاهتمام ذاته الذي بوجهه إلى التسجيلات التليفونية والمراسلات المعترضة التي يتحصل عليها فى القضايا العادية. والمشكلة الحقيقية هنا هي أن قواعد الأدلة المتعلقة بتسجيلات التليفون ورسائل البريد المعترضة هي قواعد قديمة وصارمة ومفهومة جداً لرجال الشرطة والادعاء والمحاماة، بينما لم تزل قواعد الأدلة المتعلقة بلوحات النشر قواعد جديدة ومعقدة وغير مفهومة لأحد على الإطلاق.

لقد كانت عملية sundevil أكبر حملة شهدها العالم حتى وقتنا الحالي على لوحات النشر الإلكترونية غير المشروعة، فعلى مدار أيام 7، 8، 9 مايو/ أيار 1990 تم ضبط حوالى 42 نظام كمبيوتر ومن بين الأجهزة التي ضبطت، وجد أن 25 جهازاً كانت تدير فعلياً لوحات نشر وقت الضبط.

لقد استطاعت الشرطة من خلال هذه الحملة الرائعة أن تسقط 25 لوحة نشر غير مشروعة فى ضربة واحدة. وتجدر الإشارة إلى أن الولايات المتحدة الأمريكية وحدها- تعج اليوم بما يقدر بـ 300 ألف لوحة نشر الكترونية، فإذا ما افترضنا وجود لوحة نشر واحدة من بين كل مائة لوحة نشر عاملة تدار فى أغراض غير مشروعة، سنجد أن 2975 لوحة نشر خارجة مازالت تعمل من على الأراضي الأمريكية ولم تمسها حملة sundevil الشهيرة. لقد ضبطت الحملة ما يقدر بثلث من نسبة 1٪ فقط من اجمالي لوحات نشر الكمبيوتر فى أمريكا.

لقد قام فريق متخصص من مكتب الخدمة السرية «بفونيكسش يدعمه أعضاء من مكتب المدعي العام بأريزونا ـ وهي منظمة عملية sundevil بإعداد قائمة في عام 1990 تتضمن ما لا يقل عن 300 لوحة نشر ارتأوا أنها تستحق

التفتيش والضبط. وقد كانت اللوحات الـ25 التي تم ضبطها فعلياً من بين أكثر المواقع خطورة ووضوحاً، وقد تم فحص كافة اللوحات التي تم ضبطها مسبقاً ـ قبل عملية الضبط ـ سواء بمعرفة المرشدين أو بمعرفة عملاء مكتب الخدمة السرية أنفسهم. وقد أسهم هذا الفحص المسبق فى تحديد الاحتياجات الفعلية عند الإعداد للحملة، كما ساعد في انتقاء الأشخاص المؤهلين لإنجاز العمل.

وقد كان لعملية sundevil العديد من الدوافع، نذكر منها فرصة تحقيق السبق الشرطي في مجال جرائم الاحتيال الالكتروني والحصول على كمٍّ هائل من الأدلة الإلكترونية لدراستها وفحصها وتقديمها للإدعاء.

وقد اعتبرت عملية الضبط ـ في صورتها المادية المجردة التي تمثلت في إزالة الماكينات والمعدّات ـ أجراءً هاماً خفّف كثيراً من الضغط الذي طالما تعرضت له أجهزة الإنقاذ في ذلك المجال.

لقد حرمت العملية الآلاف من لصوص بطاقات الائتمان والأطفال المتلاعبين بالأكواد من فرصة الالتقاء والتآمر والحصول على البيانات والمعلومات التي تساعدهم في تحقيق مآربهم. وبضربة واحدة جعلت عملية sundevil كل هؤلاء الأفراد صُمَّاً وعُمْياً من الوجهة الرقمية الإلكترونية.

وقد شنت أجهزة الانقاذ العديد من الهجمات المماثلة لعملية sundevil في أحياء تقطنها أغلبية من البيض الذين ينتمون إلى الطبقة المتوسطة (الفئة المشتبه فيها) مثل: مونت ليبانون- بنسلفانيا، كلارك ليك ميتشجان، وقد استهدف عدد قليل من هذه الهجمات مكاتب المشتبه فيهم بينما اتجهت الغالبية العظمى من الهجمات إلى المنازل حيث تم تفتيش غرف النوم والأبنية التي تعد بيئة مثالية لمخربى نظم الكمبيوتر.

ولم تكن عملية sundevil حملة اعتقالات ـ حيث لم يزد عدد المضبوطين فيها من الأفراد عن أربعة أشخاص ـ بل كانت حملة تفتيش وضبط. فدائماً ما لا توجد أية اتهامات إلى مخربي نظم المعلومات حتى يتم تقويم الأدلة المتوافرة في

أجهزة الكمبيوتر الخاصة بهم والتي يتم ضبطها أثناء عمليات التفتيش، وبالطبع فإن عملية تقويم أدلة الكمبيوتر تعد عملية مطولة للغاية فقد تستغرق أسابيع أو شهوراً أو أعواماً، فإذا ما تم اعتقال أحد مخربى نظم المعلومات أثناء عملية الضبط، فإن ذلك يكون لأسباب أخرى بخلاف تورطه في الجريمة الإلكترونية (مثال: إحراز مخدرات أو حيازة سلاح غير مشروع).

ودائماً ما يتعامل رجال الخدمة السرية مع مخربى نظم المعلومات على أنهم أناس أذكياء ومراوغون ولا يمكن التنبؤ بطبيعتهم أو سلوكياتهم؛ فحقيقة اختفاء المخرب وراء شاشة جهازه على مدى فترة طويلة من الوقت لا تُحسِّن من صورته بأية حال من الأحوال أو تدعونا إلى الاعتقاد بأنه «مجرد طفل». وتجدر الإشارة إلى ضرورة تعامل الشرطة وأجهزة الإنقاذ مع مخّرب نُظُم المعلومات وطوال الوقت بالقدر اللازم من الحرص.

## المبحث الثالث:
## اتجاهات التشريع اللاتيني وموقفها من جرائم سرقة المعلومات

أدى ربط الحاسبات الآلية بعضها بالبعض الآخر عن طريق شبكة المعلومات إلى سرعة انتقال المعلومات من جهة، وإلى سهولة التطفل عليها واختلاسها من جهة أخرى، عن طريق استخدام (المودم) modem [1]. حيث يسمح هذا الجهاز للمتطفلين من أي مسافة يوجدون فيها بالولوج في الحاسبات الآلية المستهدفة ومن دون أي مساس مادي بحق ملكية الغير أو ترك أي أثر يدل على انتهاك المعلومات أو نسخها. ونظراً لجسامة هذا النوع من التعدي فقد

(1) MODEM: عبارة عن أداة لترجمة تعليمات مكتوبة بلغة الحاسب الآلي إلى رموز رقمية أو العكس، حيث يسمح للحاسبات الآلية أن تستقبل وتنقل المعلومات عن طريق وسيط لخط تليفوني.

حرص العديد من الدول على إرساء مبدأ لحماية وسلامة نظم المعلومات لديها بغض النظر عن مبدأ حماية سرية البيانات المعالجة أو المتداولة.

وسوف نستعرض الحلول التشريعية التي استحدثت في هذا المجال في بعض الدول أولاً ونعرض لذلك بشيء من التفصيل، وفي القانون الفرنسي ثانياً.

## أولاً: الحلول التشريعية في بعض الدول

فى السويد تنص المادة 21 من القانون رقم 289 الصادر في 2 إبريل/ نيسان 1973 الخاص بالبيانات على أن «يعاقب.. كل من ولج بوسائل غير مشروعة إلى سجل مخصص لمعالجة البيانات آليا»؛ أي أن القانون السويدي يعاقب على مجرد الولوج فقط.

وفى الدانمارك وطبقاً للمادة 263 من قانون أول يوليه/ تموز 1985 يُعدّ من قبيل الجرائم فعل الولوج في المعلومات أو البرامج المختزنة في أجهزة المعالجة الإلكترونية للمعلومات. وتلزم المشروعات الألمانية والنرويجية بقوانين أن يكون هناك انتهاك لتدابير الأمن لملاحقة مجرد الولوج في نظم المعلومات.

## ثانياً: التشريع الفرنسي

استحدث القانون الفرنسي الصادر في 5 يناير/ كانون الثاني 1988 بموجب المادة 462/ 2 عقوبات، جريمة الولوج غير المشروع في نظم المعلومات والتي تنص على «يعاقب.... كل من ولج أو وجد بطريق الغش في كلّ أو جزءٍ من نظام مبرمج للبيانات». وتشدد العقوبة إذا ما ترتب على ذلك إلغاء، أو تعديل للبيانات التي يحتويها النظام أو إتلاف لوظيفة هذا النظام».

ويستهدف هذا النص في المقام الأول حماية الولوج في نظم المعلومات، لا حماية حق الملكية ذاته، وهو بذلك سدّ فراغاً تشريعياً هائلاً في القانون الفرنسي، ومن جهة أخرى استجاب لرغبة ملاّك الأنظمة المعلوماتية [1]

---

(1) راجع فى ذلك: J.P.Buffelan,art.Prec.P.99.

وتفترض هذه الجريمة توافر عنصرين، أحدهما مادي والآخر معنوي.

**أ ـ العنصر المادي:**

يتحقق العنصر المادي لهذه الجريمة بمجرد شروع أي شخص ـ ليس له الحق ـ في الدخول، أو تدخل بالفعل في نظام مبرمج للبيانات.

ولكن هل يشترط لنشوء الجريمة أن يكون النظام محمياً بواسطة جهاز أمن dispositif de securite؟ تمسّك مجلس الشيوخ الفرنسى بهذا الشرط، وحجته في ذلك جذب انتباه أصحاب الأنظمة إلى هذه النقطة الأساسية كى يدعموا أنظمتهم بأجهزة الأمن[1].

بينما رأت الجمعية الوطنية الفرنسية، أنه من غير المناسب التمسك بهذا الشرط، لأنه سوف يترتب عليه قَصْر الحماية الجنائية على الأنظمة المحمية بواسطة أجهزة الأمن ومن ثم يستبعد من مجال تطبيق النص أفعال الولوج التي ترتكب ضد الأنظمة المفتوحة للعامة[2] كالدليل الإلكتروني أو الخدمات التي تقدم على رقم 36 ـ 15. وكتب لهذا الرأي الأخير النجاح، وتم التصويت على النص بدون حاجة إلى اقتضاء هذا الشرط.

ويتحقق الوجود غير المشروع، بمجرد علم الشخص بأنه تدخل بمحض الصدفة أو عن طريق الخطأ ـ وعلى نحو غير مشروع ـ في نظام مبرمج للبيانات، ويستمر في حال الاتصال به بدلاً من الانفصال عنه في الحال.

وهذه جريمة من جرائم الامتناع التي يصعب تقديم دليل إثبات فيها حيث يزعم المتهم دائماً حال القبض عليه أنه كان على وشك الانفصال عن النظام المعتدى عليه[3] ويستوي أن يكون الولوج في النظام المعتدى عليه كلياً أو جزئياً

---

(1) راجع في ذلك: J.Pradel,art prec,P.827, Lucas de leyssac, OP.CIT.P.21.

(2) انظر: Rapport de r.Andre, Assemble Nationale,no.1078 «1987, 1988» P.5.

(3) راجع في ذلك: J.P.Buffelan,art. Prec,P.100.

حيث يستطيع المعتدي في حالة التدخل المقترن بالغش، أن يدعي بسهولة بأن تحوله كان محدوداً بجزء ضيق جداً من النظام، ولا يمكن التحقق من مثل هذا الإدعاء من الناحية العلمية[1].

ويقصد بالنظام المبرمج للبيانات: كل وحدة أو عدة وحدات للمعالجة والذاكرة أو البرامج أو البيانات أو وحدات الإدخال والإخراج أو الموصلات التي تساعد في الوصول إلى نتيجة محدّدة [2].

ويثور تساؤل، عما إذا كان الولوج غير المشروع يمكن أن يتحقق عن طريق ما يسمى بسرقة وقت الآلة، أي استعمال مستخدم المنشأة أو الغير ـ على نحو غير مشروع ـ للحاسب الآلي في الأغراض الشخصية.

يميل غالبية الفقه الفرنسى إلى بسط الحماية الجنائية الواردة في المادة 462/ 2 عقوبات إلى سرقة وقت الآلة[3].

**ب ـ العنصر المعنوي:**

يجب أن يتوافر لدى الفاعل قصد خلاصٍ علاوة على القصد العام «أي إتيان الفعل غير المشروع عن علم وإرادة». والذى يتمثل في نية الغش Fraudulcuscmcnt. ويقصد بالغش أن يباشر الفاعل سلوكه عن طريق الخديعة وبسوء نية وبغرض خداع الغير[4] ويتمثل قصد الغش في معرفة المتهم بأنه قد ولج أو وجد في نظام البيانات المبرمج ضد رغبة صاحب النظام وأياً كان الدافع إلى ذلك.

ولكن يثور التساؤل الآتي: هل يشكل النظام الأمني للجهاز المعلوماتي

---

(1) راجع في ذلك: F.Chamoux,art prec,H..Croze,ART,PREC V. ROULET,art prec.

(2) راجع في ذلك: J.P.Buffelan,art prec P.100.

(3) انظر في ذلك: J.Pradel,art prec,P.823,h.CROZE,ART PREC.

(4) أنظر في ذلك: Lucas de Leyssac,OP.CIT.,P.20.

عنصراً من عناصر جريمة الولوج غير المشروع في النظام المعلوماتي؟ هناك اتجاهان في هذا الصدد.

الاتجاه الأول: ويرى عدم ضرورة انتهاك نظام الأمن لكي تقوم الجريمة. ويستند هذا الرأي إلى: هل القانون، والأعمال التحضيرية له حيث تم رفض الرأي الذي كان يرى أنه من الضروري وضع تعريف لنظام المعالجة الآلية للبيانات ـ Sisteme traite ment automatise de donnees ويشترط وجود نظام أمان. لذا وأنه طبقاً لهذا الرأى فإن نظام الأمان لا يكون له إلا دور واحد، هو إثبات سوء نية من قام بانتهاك النظام والدخول بطريقة غير مشروعة، ولكن القصد الجنائي يمكن إثباته بطرق أخرى.

**الاتجاه الثاني:**

ويرى جانب آخر من الفقه ضرورة وجود نظام أمني، حيث أن القانون بجرّم الاعتداء على نظم الأمن الخاصة بالنظام المعلوماتي، ويستند هذا الرأي إلى ما يأتي:

1 ـ إن الاعتداء على النظام الأمنى يعتبر شرطاً مفترضاً في جميع الجرائم المتعلقة بنظم المعلومات.

2 ـ كما يستلزم كلاً من المنطق والعدل لهذا الشرط، حيث أن القانون الجنائي لا ينبغى أن يقوم بحماية الأشخاص الذين لا يأخذون الاحتياط اللازم المتطلب من إنسان متوسط الذكاء. فوجود نظام حماية يمكن أن يكون التزاماً مفروضاً بنص القانون على كل من يقوم بإدارة نظام معلوماتي[1].

وفى الواقع إن قبول الاتجاه الأول من شأنه أن يؤدي إلى تجريم مجرد الدخول غير المشروع، ولكن هل هذا التجريم ملائم من الناحية المنطقية والناحية القانونية؟

---

(1) راجع في ذلك: R.Gassin no.87 citant h. groze,OP.CIT,no.10

الواقع أن الأسباب المتعلقة بضرورة وضع نظام أمني في نظم المعلومات يتقتضى التفرقة بين أمرين:

الأمر الأول: حماية النظام بالمعنى الدقيق إذا وضعنا في الاعتبار مدى أهمية حماية النظام بالمعنى الدقيق والمتطلّب لتأمين النشاط الخاص بنظم المعلومات، لوجدنا أن شركات التأمين تستلزم حداً أدنى للأمن من جانب مستخدمي النظام، حيث يمكن أن يطالبوا بالتعويض؛ ومؤدّى ذلك أن القانون الجنائي يوفر حماية واسعة بالنسبة لتلك الخاصة لشركات التأمين وهذا أمر منطقي.

ومن ناحية ثانية: فإن ضرورة وجود النظام الأمني هو التزام قانوني وضروري منصوص عليه في المادة 29 من القانون الصادر في 6 يناير/كانون الثاني 1978 والخاص بنظم المعلومات والبطاقات والحريات[1].

ذلك أنّ هذه المادة تستلزم كل شخص يعمل في نطاق المعالجة الآلية للمعلومات الشخصية بضرورة اتخاذ الاحتياطات اللازمة لحفظ وحماية هذه المعلومات، وخصوصاً بمنع تشويهها أو تعديلها أو الحصول عليها بوساطة أشخاص غير مرخص لهم بالاطلاع عليها[2].

وهكذا فإن الإخلال بهذا الالتزام الخاص بوضع نظام أمني للجهاز والذي

(1) راجع في ذلك:
LOI NO-87-17 du 6-01. 78 relative Informatique aux-. Fichiers ET aux libertes J.O du 7-01.78 ET. RE etificatgif au T.O.du 25.01.78.

(2) راجع في ذلك:
Toute Personne ordonnatnt ou effectuant un traitement d informations nominatives s engage de ce Faitvis -a- VIS DES PER- sonnes concernees aprendre Toutes Precauions utiles afin de pre- sesverla Securite des information et notomment de empechet qu elles ne Soient deformees endommagees ou communiqués ades tiers non autorises.
article 29 de la loi NO.78-17.
di 6.01.78 Precitee.

يقع على عاتق مستخدم النظام المعلوماتي للمعالجة الآلية لبيانات والمنصوص عليها في المادة 29، تنطوي على جريمة جنائية معاقب عليها بالمادة 42 من قانون العقوبات الفرنسي والتي تنص على عقوبة السجن لمدة 5 سنوات.

## موقف التشريعات الانجلوسكسونية من جريمة سرقة المعلومات

سوف نتعرض في هذه النقطة لبعض النماذج التشريعية للدول الأنجلو سكسونية وذلك على النحو التالي:

### أولاً: التشريع الانجليزى في مجال جرائم إساءة استخدام النظم المعلوماتية

استحدث المشرع الانجليزى عام 1990 قانوناً يعالج فيه إساءة استخدام نظم المعلومات وقد تم بموجب هذا التشريع تجريم عملية دخول أي فرد على البيانات المختزنة بالحاسب الآلي أو البرامج، وكذلك عملية تعديلها بصورة غير مشروعة أو أي محاولة لفعل ذلك [1].

وقد نص القانون على ثلاثة جرائم محددة وهي[2]:

1 ـ الدخول المتعمّد غير المشروع: Access is deliberate and unauthorized

---

(1) راجع في ذلك:
Rapport de Mr. Andre au nom de la commission delois constitu- tiannelles de LA legistation et de l'administration generale de la republique sur la Proposition de m.Godfrain relative a la fraude informatique no. 744.P. 13. DOC. Ass.nat(1986/87) lly aura acces Frauduleux des lorsqu on cherchera a sintrodiure indumenta dans un systeme prcetege par un disposetif de Securite.

(2) وقد أدرج القانون بعض التعريفات الآتية:
ـ البيانات: هي تلك المعلومات الكائنة في صيغة قابلة للمعالجة.
ـ البيانات الشخصية: هي البيانات المتعلقة بأفراد أحياء يمكن تحديد هويتهم.
ـ الأشخاص المسند إليهم العمل في مجال البيانات: هم الأفراد المعنيّون بها.

2 ـ الدخول غير المشروع والذي يتم بنية ارتكاب العديد من الجرائم.

3 ـ قيام الفرد بأي فعل متعمد ينشأ عنه إجراء تعديل غير مشروع لمحتويات أجهزة الكمبيوتر.

ويلاحظ من صياغة هذا القانون ما يأتى:

أنّ المشرّع الانجليزى يعاقب على التآمر والشروع والتحريض.

ـ لا تُلزم جهة الادعاء أن تقدم دليلاً يستفاد منه أن الأفعال المقترفة قد استهدفت بيانات أو برامج معينة.

ـ لم يشترط القانون المشار إليه سلفاً وجود المتهم وقت ارتكاب الجريمة ولا بيانات الحاسب الآلي المستهدفة في بريطانيا.

والتفسير الواسع لقانون السرقة theft act الانجليزى يشمل التلاعب في البيانات من أجل الحصول على المنفعة المالية. فالمادة 15 من قانون السرقة الصادر سنة 1968 تنصّ على أنه «يعد مرتكباً لجريمة السرقة كل من حصل بطريق الغش أو بصفة غير مشروعة على مال يخصّ الغير بقصد حرمانه منه بصفة دائمة».

وكذلك تنص المادة الأولى من قانون السرقة الصادر سنة 1978على أنه «يعد مرتكباً لجريمة السرقة كل من حصل بطريق الغش وبصفة غير مشروعة على منفعة من الغير».

وتنص المادة 16 من القانون نفسه على أنه «يعاقب كل من حصل بطريق غير مشروع وبأى وسيلة خداع سواءٌ لنفسه أو للغير على منفعة مالية»[1].

---

(1) انظر في ذلك:
M. BRAIT,la fraude informatiqu.. une.Approche de droit compare REV. dr.pen.-cirm.p.290.

وعلى الرغم من أن ظاهر النصوص يوحي بإمكانية تطبيقها على سرقة المعلومات، إلا أن القضاء الانجليزى تردد في تطبيقها في قضية Regina v.mortiz عام 1981 والتي تتعلق وقائعها بتلاعب أحد الأشخاص في البيانات المعالجة الكترونياً بوساطة الحاسب الآلي والخاصة بسداد ضريبة TVA بهدف التهرب منها حيث اعتبرت المحكمة أن الغش الواقع على الآلة لا يعدّ من قبيل الاحتيال المعاقب عليها جنائياً، وهذا ما دفع البرلمان الانجليزى إلى إجراء تعديل سنة 1983 يهدف إلى اعتبار خداع الآلة بنيّة ارتكاب غش مالي من قبيل الاحتيال المعاقب عليه جنائياً، وهذا ما دفع البرلمان الانجليزي إلى إجراء تعديل سنة 1983 بهدف إلى اعتبار خداع الآلة بنية ارتكاب غش مالي من قبيل الاحتيال المعاقب عليه جنائياً[1] . وقد اشتمل قانون حماية البيانات الانجليزى الصادر سنة 1984 على المبادئ الآتية :

1 ـ يجب الحصول على البيانات الشخصية ـ المخزنة لأغراض المعالجة ـ بأسلوب صحيح ولتحقيق أغراض مشروعة.

2 ـ يجب حفظ تلك البيانات لأهداف محددة.

3 ـ عدم جواز استخدام البيانات الشخصية إلا للغرض المحدّد لها ولا يجوز الكشف عنها إلا بما يتفق مع ذلك الغرض المحدد لها.

4 ـ لا يجب أن تتعدى البيانات الشخصية الغرض المحدد لها.

5 ـ يجب توفير البيانات الشخصية للفرد المعني بها مع التصحيح له بإجراء أي تعديلات لازمة لها.

6 ـ يجب حفظ البيانات الشخصية بصورة آمنة تحميها من عمليات الدخول غير المشروع كما تحميها من الفقد.

(1) راجع في ذلك: m.Briat,la fraud informatique, art prec.p.290.

**الاستثناءات:**

ويستثنى من هذا القانون البيانات الشخصية المختزنة المتعلقة بالرواتب، والمعاشات، وبيانات الحسابات، علاوة على الأسماء والعناوين المخصصة لأغراض توزيع المعلومات (مثال: اتحاد البريد).

وتستثنى كذلك البيانات الشخصية المخزونة المتعلقة بمجالات الأمن القومي أو منع الجريمة أو جمع الضرائب والرسوم.

وفى حالة جمع البيانات الشخصية لأغراض التحقيق أو الأغراض الإحصائية فقط، أو حفظها كنسخة إضافية مجردة، لا يحق للأشخاص المسند إليهم العمل في مجال البيانات الاطلاع عليها، وبالرغم من وجوب تأمين البيانات الشخصية إلا أنه من الممكن أن يتم الكشف عنها لوكلاء أصحابها (مثال: المحامى أو المحاسب) أو لأحد الأشخاص العاملين لدى مستخدمى البيانات أو لأي شخص آخر في حالة وجود حاجة ملحّة لمنع وقوع إصابة أو أضرار بالصحة.

**أساليب حماية البيانات:**

وتتعدد هذه الأساليب طبقاً للقانون الانجليزي على النحو التالي:

**1 ـ الحماية عن طريق كلمة السر (كلمة المرور):**

عادة ما يتم تخزين أسماء المستخدمين وكلمات المرور في جداول، ويحفظ هذا الجدول بشكل دائم على ملف موجود على أسطوانة. وغالباً ما تحفظ جداول كلمات المرور جنبا إلى جنب مع جداول التفويض التي تحوي حقوق المستخدم فيما يتعلق بالملفات الأخرى، ويجب ألا تكون جداول كلمات المرور مشفرة على نحو «لا يمكن تعديله» وذلك لتجنب إمكانية الاطلاع على محتوياتها.

**2 ـ تشفير البيانات:**

تقوم عملية التشفير على تحويل الرسالة من نص واضح إلى نص مشفَّر، ويتم إرسال الرسالة المشفّرة عبر قناة اتصال، حيث يقوم الحاسب المتلقي بفك شفرة الرسالة.

**التدابير الأمنية الأخرى:**

بخلاف كلمة المرور، يمكن التعرف على المستخدم المصرح له وذلك عن طريق:

- التعرف على بصمة العين.
- التعرف على بصمات الأصابع.
- التعرف على الصوت.
- التعرف على الوجه:

## ثانياً : التشريع الأسترالي:

تبنت غالبية الولايات في أستراليا تفسيراً واسعاً لمفهوم السرقة مستوحى من القانون الانجليزي. ويبدو ذلك واضحاً في قضية، حيث أدانت إحدى المحاكم الأسترالية شخصاً بجريمة السرقة لاحتياله على مدير أحد البنوك في سيدنى حيث أنه تلاعب في برامج الحاسب الآلي كي تبدو الاعتمادات المالية في صالحه[1].

ويختص قسم جرائم الكمبيوتر التابع للبوليس الفيدرالي الاسترالي والذي تكوَّن عام 1989 بمهمتين رئيسيتين ـ المهمة الأولى هي البحث والتقصي وجمع المعلومات الاستخباراتية عن جرائم محددة من جرائم الكمبيوتر، بينما المهمة الثانية هى توفير الدعم الفني لوحدات البحث والتحقيق السري المنهمكة في

(1) راجع في ذلك: m.Briat,la fraude informatique,art prec.p.291.

التحقيق في الجرائم المتصلة بالكمبيوتر أو التي تعتمد عليه في ارتكابها.

والتشريع الذى يحدد مسؤولية البوليس الفيدرالى الاسترالي بشأن جرائم الكمبيوتر المحددة يوجد في قانون العقوبات لدول في الكومنولث والصادر عام 1914 (الجزء6أ) والذي يشمل الأقسام من 76 أ إلى 76ف. هذه الأقسام المتعلقة بالأفعال الإجرامية تشمل قائمة بالظروف والملابسات التي تشكل فعلاً إجرامياً ودرجة العقوبة المحتملة المرتبطة بهذه الأفعال. وقد تم وضع هذا التشريع في يوليو 1989 وتم تعديله في 1991. ولدى البوليس الفيدرالي الاسترالي الحق السيادي لتطبيق هذا التشريع في أحد موقفين:

الموقف الأول: كان الكومنولث يتمتع بالسلطة والحق في تطبيق هذا التشريع حينما كان الفعل الإجرامي موجهاً نحو الكمبيوتر التابع للكومنولث، أو أحد أجهزة الكمبيوتر التي تحتوي على بيانات أو معطيات لصالح الكومنولث. والإشارة إلى البيانات أو المعطيات التي تم تخزينها في الكمبيوتر لصالح الكومنولث تشمل الوضع حينما يتم تخزين هذه البيانات والمعلومات بناءً على توجيه أو طلب من الكومنولث.

الموقف الثاني: يمكن تطبيق هذا التشريع حينما يكون الفعل الإجرامي موجهاً ضد أي كمبيوتر بوساطة أي تسهيل يتم تشغيله أو توفيره بمعرفة الكومنولث أو بمعرفة أي طرف وسيط. وتعريف الوسيط أمر واسع النطاق وهو يشمل المنظمات كافة، سواء الخاصة أو الحكومية، التي تقوم بتزويد هذه الخدمة بموجب ترخيص ممنوح طبقاً لقانون الاتصالات عن بُعد الصادر عام 1991.

وبصفة أساسية نبين فيما يلي الفئات الأربع للأفعال الإجرامية الواردة في هذا التشريع.

الفئة الأولى: هي الأفعال الإجرامية الخاصة بالكمبيوتر التي تتعلق

بالوصول غير القانوني للكمبيوتر والحد الأقصى للعقوبة عن هذا الفعل هي الحبس لمدة 6 أشهر.

الفئة الثانية: من الأفعال الإجرامية الخاصة بالكمبيوتر تتعلق بالوصول غير القانوني لأحد أجهزة الكمبيوتر بقصد خداع شخص معين والتدليس عليه والحد الأقصى للعقوبة عن هذا الفعل هي الحبس لمدة سنتين.

الفئة الثالثة: من الأفعال الإجرامية تتعلق بالوصول غير القانوني إلى أجهزة الكمبيوتر والاطلاع على أنواع معينة من البيانات والمعلومات.

الفئة الرابعة: من هذه الأفعال الإجرامية أنها تطابق نوعين معينين من الآثار المترتبة على نظام الكمبيوتر التي ترقى لمستوى الفعل الإجرامي حينما يتم التسبب في هذه النتائج عن عمد.

**ثالثاً: التشريع الكندي:**

استحدث قانون العقوبات الكندي[1] المادة 301 فقرة 2 والتي تنص على:

أ - كل من حصل بطريق الغش وبدون وجه حق مباشرة أو بطريق غير مباشر على خدمات من حاسب آلي.

ب - كل من ولج بنية الغش، بواسطة جهاز الكتروني أو صوتى أو آلي مباشرة أو بطريق غير مباشر في حاسب آلي.

جـ - كل من استعمل حاسباً آلياً مباشرة أو بطريق غير مباشر بغرض ارتكاب جريمة منصوص عليها في الفقرة أ،ب أو جريمة منصوص عليها في المادة 387 خاصة ببيانات أو حاسب آلي يعد مرتكباً لفعل إجرامي ويعاقب بالحبس لمدة عشر سنوات.

وتنص المادة 387: يُعدّ مرتكباً لعمل آثم كل من باشر عمداً:

---

(1) راجع في ذلك: Vivant et le stanc, lamy informatique no.2489.

أ ـ إتلاف أو تعديل البيانات.

ب ـ سرقة البيانات أو جعلها غير صالحة أو عديمة الفائدة.

جـ ـ منع أو إعاقة الاستخدام المشروع للبيانات.

د ـ منع أو إعاقة شخص في استخدام حقه المشروع للبيانات أو رفض ولوج شخص له الحق في البيانات.

**ثالثا: التشريع الأمريكى:**

يطبق في الولايات المتحدة الأمريكية القوانين الخاصة بالغش في مجال البنوك والبريد والتلغراف والاتفاق الإجرامي لأغراض ارتكاب الغش على جرائم سرقة المعلومات. بل إن بعض الولايات الفيدرالية أصدرت قوانين بموجبها أعطت مفهوماً واسعاً للمال بحيث يشمل «كل شيء ينطوى على قيمة» ويندرج تحت هذا التعريف الأموال المعنوية والبيانات المعالجة، وتعاقب هذه القوانين على الاستخدام غير المسموح به بغرض ارتكاب أفعال الغش أو للاستيلاء على المال[1] وعلى المستوى الفيدرالي صدر قانون الولوج المصطنع في الحاسب

---

(1) استحدثت الولايات الأمريكية «مثل أريزونا وكاليفورنيا وكولورادو وديلادار وفلوريدا وجورجيا وإلينوى وميتشجان وميسوري ومونتانا وأوتاوا ونيومكسكو. . .) العديد من القوانين الجنائية التى تعاقب على الاستخدام غير المسموح به للحاسب الآلي بغرض الاحتيال أو الحصول على مال، والمجال هنا ليس متسعاً لفحص جميعها، ولذا نكتفي بإيراد ملاحظتين عليها:

أولاهما: أن آلبات التجريم في هذه القوانين على درجة كبيرة من الاختلاف ويبدو ذلك من زاويتين:

(أ) أن جميع هذه القوانين إذا كانت تتمسك بضرورة توافر الغش أو سوء النية في الأفعال المعاقب عليها إلا أن صيغتها في هذا الشأن جاءت غير مطابقة، وعلى سبيل المثال فقانون كاليفورنيا ينص على أن «يعاقب كل شخص ولج عن عمد أو سوء نية. . . .» مادة 502 من قانون عقوبات كاليفورنيا الصادر سنة 1979 والمعدل سنة 1982 «وقانون ديلادار» ينصان على «كل من. . . . وكان ذلك عن تبصر أو تروٍّ مباشر أو بطريق غير مباشر» مادة 558 والمعدلة في سنة 1982، وقانون فلوريدا ينص على «كل من باشر. . . . عن تروٍّ وعلم وبدون إذن. . . . . .«وقانون 1978 =

الآلى في أكتوبر سنة 1984[1]، counterfeit access device and computer

---

= وقانون بنسلفانيا «ينص على «كل من. . . . عمداً وبدون إذن» قانون سنة 1983».

(ب) أن بعض هذه القوانين مال إلى تقنين، وبشكل مختصر، الأفعال المجرمة مقتدياً في ذلك بالنموذج الفيدرالى ومنها قانون كاليفورنيا والذى يعاقب «كل من ولج عمداً في نظام أو شبكة معلوماتية بغرض محاولة أو تنفيذ أي مؤامرة أو حيلة بغرض الحصول على نقود أو خدمات»؛ قانون العقوبات مادة 502/ ب «ويجرم هذا القانون أيضاً «كل من ولج وبسوء نية في نظام شبكة معلوماتية بغرض الحصول على معلومات غير مسموح بها تتعلق بسمعة الغير أو كل من أدخل معلومات مصطنعة بغرض تحسين أو إساءة سمعة الغير ويعاقب أخيراً كل شخص ولج بسوء نية وأتلف أو محا أو أضرّ بأي نظام معلوماتي أو شبكة معلوماتية أو كيان منطقى أو بيانات. وعلى النقيض تنبت بعض القوانين الأخرى المنهج التحليلى ومنها على سبيل المثال قانون فلوريدا والذي احتوى على ثلاث مجموعات أساسية إحداها: مخصصة للجرائم التى تقع على البيانات الموجودة بالبرامج، والثانية: خاصة بالجرائم التى تقع على المعدات والتجهيزات المعلوماتية، والثالثة : خاصة بجرائم المستخدمين لنظم المعلومات، ولكل مجموعة منها قواعدها الداخلية الخاصة بها وثانيتهما: تتعلق بالمنهج الانجلو سكسونى في التعاريف القانونية حيث يلاحظ أن هذه التعاريف ليس لها أية قيمة خارج الولايات المتحدة، بل وأيضاً خارج الولاية التي تنص عليها، وفضلاً عن ذلك فليس لها أية قيمة خارج النص الذى يحتويها حيث أنها تعطى من أجل احتياجات النص.

راجع في ذلك: Vivant et le stanc, lamy droit de informatique,no.2487.

(1) بدأت ـ أنفينا سيكوريتى كورب ـ في بادئ الأمر وكأنها شركة انترنت نموذجية، بمكاتبها وحاسباتها وموظفيها ونظامها الأمنى الحاسوبي، ولم يكن ينقصها سوى الزبائن. لكن تبين الآن أن تلك الشركة التى بدت مشروعاً فاشلاً للوهلة الأولى كانت شركة وهمية أنشاها مكتب التحقيقات الفيدرالية الأميريكي (اف. بى آي) للإيقاع بشابين روسيين متهمين باختراق كمبيوترات شركات إنترنت أمريكية واختلاس معلومات حساسة في محاولة لابتزاز المال. وتقول السلطات إن اليكسى ايفانوف (21 عاماً) وفاسيلى جورشكوف (25 عاماً) وكلاهما من مدينة شليابنسك الروسية قد ابتلعا الطعم ووقعا في فخ الإف بى آي. وفى حين رفض مكتب التحقيقات الفيدرالية الإدلاء بأية تعليقات، فإن وثائق قضائية كشف عنها النقاب أخيراً تبدو وكأنها رواية جاسوسية يروى فيها عملاء الإف بى آي كيف تمكنوا من الإيقاع باللصين عن طريق إنشاء شركة زائفة ودعوة ايفانوف وجوشكوف لمحاولة اختراق أنظمتها الحاسوبية المحصنة، وبعد أن نجح القرصانان الروسيان في اختراق الأنظمة عن بعد، وجه موظفو شركة أنفيتا دعوة لهما للقدوم إلى سياتل في الولايات المتحدة لمناقشة إبرام عقد شراكة واستعراض كامل امكانياتهما في مجال التسلل إلى أجهزة الكمبوتر عبر الانترنت، وبينما كان الشابان يستعرضان =

Fraud and abuse act والذى ولج عمداً في حاسب آليّ بدون إذن، أو كان مسموحاً بالولوج منه، واستغل الفرصة التي سنحت له عن طريق هذا الولوج لأغراض لم يشملها الإذن، وقام عمداً عن طريق هذه الوسيلة باستعمال أو تعديل أو إتلاف أو إفشاء معلومات مختزنة في الحاسب متى كان هذا الأخير يعمل باسم ولصالح الحكومة الأمريكية، وطالما أثرت هذه الأفعال على أداء وظيفته. ويمكن لهذا النص وبطريق غير مباشر وبشروط معينة، أن يشمل النّصْب الذى يرتكب عن طريق الحاسب الآلي، ولكن وزارة العدل الأمريكية قدمت في أغسطس/آب سنة 1984[1] مشرًوعا بقانون يستهدف مباشرة حالة الغش المعلوماتي والذى يعاقب «كل من رتّب أو صمّم خطةً ما أو حيلة بغرض ارتكاب غش أو الاستيلاء على مبلغ من النقود أو مال لا يخصّه، وولج أو حاول الولوج في حاسب آلي بغرض تنفيذ أو محاولة تنفيذ هذه الخطة أو الحيلة أو لارتكاب أو محاولة ارتكاب مثل هذا النصب أو هذه السرقة أو الاختلاس. . . » ومصطلح المال property وفقاً لهذا المشروع بقانون يشمل «كل الوسائل المالية

---

= مهاراتهما في الشراكة الوهمية استخدم إلاف بى آي تقنية تنصت حاسوبية تبسط نشاطها عبر الإنترنت وتخترق النظام الحاسوبي الخاص بالمتهمين في روسيا.

ويقول خبراء أمن الإنترنت أن القضية تعرض لمدى تطور مقدرات مكافحة جرائم الإنترنت لدى مكتب التحقيقات الفيدرالية لكن الدفاع يثير الاستفهام حول مشروعية استخدام هذه الأساليب.

راجع في ذلك: جريدة البيان ـ دبي ـ الإمارات العربية المتحدة، العدد 7633 تاريخ 12 مايو/أيار 2001.

(1) صدر في الولايات المتحدة الأميركية القانون الفيدرالى بشأن الغش والعبث المعلوماتي computer fraud & abuse act في عام 1984 وأدخل عليه تعديلات كان آخرها عام 1996. ويواجه هذا القانون عدة أفعال تتصل بالدخول غير المشروع أو الحصول متجاوزاً التصريح على معلومات تتعلق بالدفاع الوطنى أو العلاقات الخارجية لا يجوز الكشف عنها. ويعاقب أيضاً على نقل مكونات لبرامج أو معلومات دون موافقة من صاحب الشأن في حالة ما إذا ترتب على هذا النقل خسائر لشخص أو أكثر، ويواجه القانون أيضاً مشكلة غش كلمات المرور بما يمكن مرتكبه من الدخول على نظام للكمبيوتر إذا كان من شأنه الإضرار بالتجارة بين الولايات بالتجارة الخارجية. راجع في ذلك: د. طارق سرور، سبقت الإشارة إليه، ص53.

والمعلومات التي تحتوي على بيانات معالجة والمكونات الالكترونية والكيانات المنطقية وبرامج الحاسب الآلي سواء بلغة الآلة أو بلغة مقروءة للإنسان وكل قيمة أخرى ذات طابع مادي أو معنوي»[1].

وقد خوّل الكونجرس الأمريكى[2] قطاع الخدمة السرية سلطة التحقيق في عمليات الاحتيال التي تتم عبر الشبكات والتي تعرف باسم «عمليات التحايل على وسائل الدخول للمعلومات. وذلك بموجب البند رقم 18 من قانون الولايات المتحدة الأميركية القسم 1029 ويضم القسم المذكور تعريفاً عاماً لمصطلح وسائل الدخول للمعلومات وهو:

«أية بطاقة أو لوحة أو رقم كوديّ أو رقم حساب أو أية وسيلة أخرى من وسائل الدخول على الحسابات بغرض التحصل على أموال أو بضائع أو خدمات أو أي شيء آخر ذو قيمة يمكن استخدامه كوسيلة من وسائل بدء نقل الأموال».

ومن هنا نرى أن المصطلح يمكن أن يتسع بحيث يشمل بطاقات الائتمان وأرقام حساباتها وكذا بطاقات الشحن الهاتفية، وأكواد الدخول على التليفونات. ويلاحظ على نصّ القسم 1029 أنه وقد منح قطاع الخدمة السرية سلطة ومباشرة في مواجهة ذلك «العالم الرقمي الخفي» دون أن يشير من قريب أو بعيد لكلمة كمبيوتر.

ويتوافر العديد من وسائل الاحتيال القياسية التي تعرف باسم «الصناديق الزرقاء» وتستخدم لسرقة الخدمات التليفونية من أجهزة المفتاح الآلي القديم وبالطبع فإن مثل هذه السرقات تعد من بين عمليات «الاحتيال باستخدام وسائل

---

(1) راجع في ذلك:
Mendes «m.w» la legislation penale en matiere d ordinateurs et les measures de securite aux ETATS-Unis, Droit de informatique mumero special 1985.p.41.

(2) انظر في ذلك:
The Hacher crackdown law and Disorder on the Electronic fron - tier by Bruce sterling p.0172,1994.

الدخول للمعلومات». بفضل أحكام القسم 1029، لم يقتصر الأمر على الإقرار بعدم مشروعية عمليات «استخدام وسائل دخول» مزيفة، بل امتد ليشمل عمليات تخليقها. كذلك فقد أدرجت عمليات «الإنتاج» و«التصميم» و«النسخ» و«الجمع» الخاصة «بالصناديق الزرقاء» ضمن الجرائم الفيدرالية.

وتعد ماكينات الصرف الآلية ـ التي انتشرت في سائر أرجاء الولايات المتحدة الأمريكية خلال حقبة الثمانينات ـ من بين «وسائل الدخول للمعلومات» وتعتبر أية محاولة للمسها بالضغط على لوحة مفاتيحها، أو التلاعب في البطاقات البنكية البلاستيكية مثيلَ فعلٍ يندرج تحت طائلة العقوبات المدرجة بالقسم 1029.

ويتسم القسم 1029 بالمرونة والوضوح؛ فإذا ما افترضنا عثور أحد الأشخاص على كلمة المرور الخاصة بإحدى أجهزة الكمبيوتر داخل صندوق قمامة شخص آخر!! فإن كلمة المرور هذه تعتبر «كود» أو «وسيلة دخول على الحساب». وكذا إذا ما افترضنا أن أحد الأشخاص قد تمكن من الدخول على أحد أجهزة الكمبيوتر وقام بنسخ بعض البرامج المخزونة عليه لحسابه الخاص، فهو بذلك قد حصل على «خدمة» «خدمة جهاز كمبيوتر» وكذا «شيء ذي قيمة» (البرنامج المنسوخ) دون وجه حق. وأخيراً، إذا ما افترضنا أن أحد الأشخاص قد قام بإطلاع مجموعة من أصدقائه على كلمة المرور التي عثر عليها أو سرقها، وتركهم أو شجعهم على استخدامها فهو بذلك «يتاجر في وسائل الدخول غير المشروعة».

ويشتمل القسم 1029 على بندين:

أولهما: ضرورة تأثير الجرم على التجارة الداخلية أو الخارجية للدولة كي تقع تحت طائلة ونطاق الاختصاص الفيدرالى.

وثانيهما: يتعلق بحجم المال، فهناك قاعدة تقضى بعدم قيام المسؤولين الفيدراليين بتتبع المجرمين المتورطين في جمع مبالغ بسيطة من المال. حيث أن

الجرائم الفيدرالية يجب أن تتسم بالخطورة، ويحدد القسم 1029 الحد الأدنى للخسارة المالية التي تقع تحت طائلة القانون الفيدرالى بمبلغ ألف دولار أمريكى.

وقد منح القسم 1030 الخاص بـ «الاحتيال والأنشطة ذات الصلة المرتبطة بالكمبيوتر» منح قطاع الخدمة السرية السلطة القانونية المباشرة على الأعمال المتصلة باختراق الكمبيوتر كافة.

## المبحث الرابع:
## مكافحة الجريمة الرقمية والمعلوماتية في الغرب

اقتناعاً بالحاجة إلى تحقيق سياسة جنائية مشتركة، رأت الدول الأعضاء في المجلس الأوروبي، وبعد التوصيات التي تقدمت بها اللجنة الأوروبية حول مشكلات الجريمة في مجال جرائم الكمبيوتر، تمّ توقيع الاتفاقية الأوروبية بشأن جرائم الكمبيوتر، بتاريخ 23/ 11/ 2001م بغرض حماية المجتمع الأوروبي من جرائم الكمبيوتر وذلك من خلال التقريب بين التشريعات القانونية الجزائية ولتمكين وسائل التحقيق الفعالة فيما يتعلق بهذه الجرائم، وفتح الباب أمام أكبر عدد ممكن من الدول لكي تصبح أطرافاً في الاتفاقية لحاجة المجتمع إلى نظام سريع وفعال للتعاون الدولي،والذي يأخذ بعين الاعتبار المتطلبات المحددة لمكافحة جرائم الكمبيوتر.

وتتكون هذه الاتفاقية من 48 مادة مقسّمة إلى أربعة فصول على النحو التالي:

الفصل الأول يتضمن تعريفاً للمصطلحات الواردة في الاتفاقية، ومنها تعريف بنظام الحاسوب والذي يعني أي جهاز أو مجموعة من الأجزاء المتصلة فيما بينها، أو أية أجهزة أخرى ذات علاقة، والتي يقوم واحد أو أكثر منها، بحسب برنامج ما، بالمعالجة الأوتوماتيكية للبيانات، كما بين هذا الفصل ما

المقصود ببيانات الحاسوب، وهو أي عرض أو تمثيل للحقائق أو المعلومات أو الأفكار بشكل ملائم لمعالجتها في نظام الحاسوب،بما في ذلك أي برنامج ملائم يؤدي لقيام نظام الحاسوب بالعمل وأداء وظيفة ما، وكذلك عرف مزود الخدمة بأي جهة عامة أو خاصة توفر لمستخدمي خدماتها القدرة على الاتصال بطريق نظام الحاسوب، أو أي جهة أخرى تعالج أو تخزن بيانات الحاسوب بالنيابة عن جهة الاتصال أو مستخدمي تلك الخدمة، كما عرف مرور البيانات، بمعنى أي بيانات حاسوب متعلقة بأي اتصال بطريق نظام الحاسوب،ينشئها نظام الحاسوب يشكل جزء من سلسة اتصال، تشير إلى منشأ الاتصال أو اتجاهه أو طريقه أو وقته أو بياناته أو حجمه أو مدته أو نوع الخدمة أساساً.

أما الفصل الثاني من هذه الاتفاقية فيقع تحت عنوان الإجراءات الواجب اتخاذها على المستوى الأوروبي والوطني والمتمثلة في أن تتبنى التشريعات الجنائية الوطنية (قانون العقوبات العام) للدول الأعضاء في الاتفاقية جرائم ضد سرية وسلامة وتوفر بيانات وأنظمة الحاسوب، كالدخول غير المشروع والتدخل غير المشروع وتشويش البيانات وتشويش النظام وإساءة استخدام الأجهزة والتزييف المرتبط بالحاسوب والاحتيال، والجرائم المرتبطة بالصور الإباحية للأطفال والجرائم المرتبطة بالتعدي على حقوق الطبع والحقوق الأخرى ذات العلاقة والمسؤولية والعقوبات الإضافية. ومن جانب آخر أن تتبنى الدول الأعضاء في قانون الإجراءات الجنائية تحديد السلطات والإجراءات الواردة في الاتفاقية بغرض إجراء التحقيقات والإجراءات الجنائية المحددة، وكذلك تبيان الشروط واحتياطات الأمان المتمثلة في توفير الحماية الكافية للحقوق وحريات الإنسان، بما في ذلك الحقوق الناشئة عن أي التزامات أخذتها الدول الأعضاء على عاتقها بموجب اتفاقية المجلس الأوروبي لعام 1950م، حول حماية حقوق الإنسان والحريات الأساسية،والعهد الدولي للحقوق المدنية والسياسية لعام 1966م وأي أدوات دولية حول حقوق الإنسان.

وكذلك أكدت الاتفاقية على ضرورة تحديد الاختصاص بشأن أي جريمة وردت وفقاً لأحكام هذه الاتفاقية، عندما ترتكب الجريمة على إقليم الدولة الطرف في الاتفاقية أو على متن سفينة ترفع علمها، أو على متن طائرة مسجلة بموجب قوانينها أو من قبل أي من مواطنيها، إذا كانت الجريمة معاقب عليها بموجب قانونها الجنائي أو إذا ارتكبت الجريمة خارج الاختصاص الإقليمي لأي دولة.

كما حددت الاتفاقية في الفصل الثالث منها المبادئ العامة المتعلقة بالتعاون الدولي والمتمثل في تطبيق الأدوات الدولية ذات العلاقة حول التعاون الدولي في الشؤون الجنائية والإجراءات المتفق عليها على أساس التشريع الموحد أو المتبادل والقوانين المحلية،إلى أقصى مدى ممكن لأغراض التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المرتبطة بأنظمة وبيانات الحاسوب أو لجمع الأدلة بشكلها الإلكتروني في جريمة جنائية، إضافة إلى ذلك الإشارة إلى المبادئ المتعلقة بالتسليم في الجرائم الجنائية الواردة في الاتفاقية بشرط أن تكون معاقب عليها بموجب قوانين كلا الطرفين المعنيين بسلب الحرية لمدة أقصاها سنة واحدة على الأقل أو بعقوبة أشد.

وكذلك الجرائم الجنائية التي يجب أن يتم اعتبارها قابلة للتسليم،أو إذا كان هناك طرف يجعل التسليم مشروطاً بوجود اتفاقية تسليم، ثم تلقى طلب تسليم من طرف آخر ليس لديه اتفاقية تسليم معه،فيجوز له أن يعتبر هذه الاتفاقية أساساً قانونياً للتسليم فيما يتعلق بأي جريمة جنائية أُشير إليها في الاتفاقية.

كما وضعت الاتفاقية مجموعة من المبادئ العامة المتعلقة بالمساعدة المتبادلة لأغراض التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المرتبطة بأنظمة وبيانات الحاسوب، أو لجمع الأدلة بشكلها الإلكتروني في أية جريمة جنائية، كما بينت الإجراءات المتعلقة بطلبات المساعدة المتبادلة في غياب الاتفاقيات الدولية القابلة للتطبيق.كما استخدمت الاتفاقية مصطلح الشبكة بمعنى

أن على كل طرف أن يعين نقطة اتصال متاحة بواقع (24) ساعة في اليوم سبعة أيام في الأسبوع، لضمان توفير المساعدة الفورية لأغراض التحقيقات أو الإجراءات في الجرائم الجنائية المرتبطة بأنظمة الحاسوب والبيانات، أو لجمع الأدلة بشكلها الإلكتروني في جريمة جنائية، مثل هذه المساعدة ستشمل، إذا سمح بذلك القانون المحلي والممارسة، تسهيل أو القيام مباشرة بما يلي:

أ - توفير المساعدة الفنية.

ب - حفظ البيانات وفقاً لما نصّت عليه الاتفاقية.

ج - جمع الأدلة وإعطاء المعلومات القانونية، وتحديد المشتبه بهم.

واختتمت الاتفاقية الفصل الرابع بأحكام نهائية والتي تضمن العديد من الأحكام ومن ضمنها إجراء مشاورات بين الأطراف بشكل دوري من أجل تسهيل الأمور التالية:

أ - الاستخدام والتطبيق الفعال لهذه الاتفاقية بما في ذلك تحديد أي مشكلات تعترض سبيلها، وكذلك تأثيرات أي تصريح أو تحفّظ تمّ وفقاً لها.

ب - تبادل المعلومات حول التطورات القانونية أو التكنولوجية الهامة أو حول السياسة المتعلقة بجرائم الحاسوب وجمع الأدلة بشكلها الإلكتروني.

ج - دراسة إمكانية استكمال أو تعديل الاتفاقية.

بهذا نرى أن هذه الاتفاقية تعد أول وثيقة قانونية دولية (أوروبية) تعتمد تدابير وأحكاماً حول جرائم الحاسوب والتي جسدّت القلق البالغ الذي يساور الدول الأطراف، إزاء جسامة وخطورة جرائم الحاسوب، ومؤمنة بأن العمل الفعّال ضد جرائم الحاسوب يتطلب تعاوناً دولياً متزايداً وسريعاً وفعالاً في الأمور الجنائية وكذلك الحاجة لحماية المصالح المشروعة في استخدام وتطوير تكنولوجيا المعلومات.

## الفصل الخامس

# الجرائم الرقمية والإنترنت في القوانين الوطنية المقارنة

يركز هذا الفصل على تبيان موقع جرائم الإنترنت ـ على وجه الخصوص ـ في التشريعات المقارنة من خلال سبعة مباحث، ركّز الأول منها على جريمة العدوان على الإئتمان الرقمي، فيما تناول المبحث الثانى جريمة الاحتكار والاحتكار المضاد، وتناول المبحث الثالث جرائم الأخلاق، وتحدث المبحث الرابع عن جريمة الترويج السمعي ـ المرئي الفاضح، واختص المبحث الخامس بجريمة البث العلني وتشمل النشر والسبّ والقذف والتشهير والمراسلة، وجاء المبحث السادس متناولاً جريمة المطاردة والإزعاج.

## المبحث الأول:
## جريمة الاعتداء على الائتمان الرقمي

يعني الائتمان Credit إضافةً مستقبليّةً للأموال المشمولة بالحماية بحيث تضمن هذه الإضافة كل التصرفات المالية للشخص. والمبدأ الأساسي في الائتمان هو الحماية، إذ برز الائتمان على إثر تصاعد حدة جرائم السرقة بالإكراه، والتي وصلت إلى أعلى معدلاتها في العدوان على الحياة في مقابل

نهب المال من الضحايا. فالهدف يظل هو اختلاس الأموال، إلا أن السارق فضلاً عن كونه يستخدم الإكراه، فإنه كذلك يفضّل ألا يترك أثراً وراءه يمكن أن يقود إليه.

وعلى الرغم من كون قاعدة الحماية هي الأموال، فإن الجريمة استطالت أيضًا الائتمان لكون إن الأموال عبر الائتمان تتحول إلى أرقام موضوعة على بطاقات (كُروت) يتسلّمها المؤتمَن من المصرف الذي يتعامل معه.

ومن حيث الطبيعة فإنه يميَّز في شأن الائتمان بين التعامل به في العالم المادي وبين التعامل به عبر الإنترنت. فهو في عالمنا المادي يُعد وسيطًا لكونه يحلّ محلّ النقود في التعامل، حيث أنه عبر الإنترنت لا يمكن اعتباره وسيطًا، وإنما هو أحد أشكال السَّداد كالنقود تمامًا. ذلك إن ما يتم عرضه للسداد عبر الإنترنت ليس «الكارت» الذي يثبت وجود الائتمان وإنما رقم التعامل الائتماني الموضوع على «الكارت» ويسدد به الثمن.

وبتطور التقنية في ظل ثورة المعلومات نشط الائتمان، سيما عبر التجارة الإلكترونية/ الإنترنت على وجه التحديد. فالتعامل المالي عبر الإنترنت كما استطاع استيعاب فكرة ظهور أشكال جديدة للنقود، فإنه كذلك يستطيع استيعاب فكرة الائتمان، خصوصاً إذا علمنا أن التعامل بالائتمان عبر الإنترنت له سوابق تاريخية. إذ يكفي أن تضع اسمك ورقم بطاقة الائتمان الخاصة بك لكي تصل إلى مُبتغاك أو غرضك التجاري، كالبيع والشراء، والاشتراك في مؤسسات وأندية. . .الخ. ويمتد نشاط التعامل بهذه البطاقات إلى النواحي العالمية؛ إذ يجوز اختراق الحدود بمقتضى الائتمان[1] أو بالأحرى تقلص فكرة رقابة الدولة عليها[2].

(1) د. حازم الببلاوي: النظام الاقتصادي الدولي المعاصر، عالم المعرفة، العدد 257/ الماء/ مايو 2000، الكويت، ص154.
(2) المرجع السابق، ص165.

وفي الفقرات التالية سوف نتعرض لموقف عدد من التشريعات المقارنة من هذه الجريمة ونتطرق بعد ذلك لمظاهر العدوان على الائتمان عبر الإنترنت.

**أولاً: الجريمة في التشريع المقارن:** كان التشريع الفرنسي من أوائل التشريعات التي قررت سلوك المسلك الجنائي حال العدوان الإجرامي على بطاقات الائتمان، وذلك منذ عام 1988 بقانون Godfrain (نسبة إلى النائب الذي تقدم بمشروع القانون إلى الجمعية الوطنية) المؤرخ 5/ 1/ 1988، وهو القانون الذي أضيف إلى نص المادة (5 ـ 462 عقوبات فرنسي جديد) بشأن الاحتيال على بطاقات الائتمان. ومما تجدر الإشارة إليه أن الاحتيال المذكور Faux قد تولى المشرّعُ الفرنسي تفسيره على ضوء المادة (1 ـ 441 ـ عقوبات فرنسي جديد). ويشار هنا إلى القانون المؤرخ 30 سبتمبر/ أيلول 1991 المعدِّل للمرسوم المؤرخ 30/ 10/ 1935 بإصدار قانون الصك، قد أضاف موادَّ تتعلق ببطاقات الائتمان وذلك بالعقاب على تقليد Contrfacon وتزييف Falsification هذه البطاقات.

**ثانياً: مظاهر العدوان على الائتمان عبر الإنترنت؛** تتخذ أشكال العدوان على الائتمان عبر الإنترنت أحد شكلين:

**(أ) الاستيلاء على أرقام كروت الائتمان:** إذ أن لكل كارت ائتمان عنوانًا فرديًا خاصًا ID number يتميز به عن غيره، تمنحه المؤسسة المالية للمشترك لديها في هذه الخدمة بحيث تحل محل التعامل بالأموال السائلة.

والشكل المادي لكروت الائتمان يتمثل في تلك البطاقات البلاستيكية الموصوفة بمقاييس معينة، وأما نطاق استخدامها فيختلف بحسب نوعية الخدمة التي تستخدم فيها. فكما أن هناك بطاقات تستخدم لسحب مبالغ مالية من آلات توفرها المؤسسات المالية التي تُصدر هذه البطاقات، فإنه أيضًا تتوافر خدمة التعامل بالبطاقة مباشرة في الحياة الاقتصادية من خلال رقم البطاقة.

ولقد امتدّ نشاط بطاقات الائتمان إلى الإنترنت فانفتح المجال لها لكي

تضع عملية استخدامها على محكّ بدرجة عالية من الخطورة إزاء مظاهر الاحتيال التي يتم بها الاستيلاء على أرقام هذه البطاقات بشكل غير مشروع، وعلى النحو الذي يحقق تكامل جريمة الاستيلاء على بطاقات ائتمان.

وعلى الرغم من أن الاستيلاء على بطاقات الائتمان عبر الإنترنت يكون بغرض الحصول على سلع وخدمات يتم سَداد مقابلها المادي من بطاقات الائتمان المختلسة، إلا أن موضوع اختلاس بطاقات الائتمان لا يشكل سرقةً ماديةً أساسًا وإنما يكون عدوانًا على الائتمان تحديدًا باستغلال قيمة الضمان من قِبل مَن ليس له الحق فيه، إذ أن المال المضمون بالائتمان لم تخرج حيازته ماديًا على وجه التحديد، وإنما كل ما في الأمر أنه يتم إنفاقه لصالح الغير ممن لا يجوز له إنفاقه دون إرادة صاحبه. وعليه فنقطة التفاعل في الائتمان هي مسألة الإنفاق ومدى جوازه، وليس الحيازة المادية كما السرقة. ويفيد الائتمان في منطق الإنفاق عبر الإنترنت عدم لزوم الحضور المادي لأشخاص التعامل المالي وهو ما يطلق عليه البعض مصطلح «Carding» والذي يفيد الاستخدام غير المصرح به لكارت الائتمان من قبل مالكه[1]. ومن ثم فإن ما تتم سرقته عبر الإنترنت ليس هو بطاقة الائتمان لعدم توافر الوسيلة المادية وإنما فقط كود البطاقة. لذلك يطلق على هذه الجريمة أحيانًا مصطلح سرقة الهوية «Identity theft».

وعلى الرغم من أن اتجاهًا فنيًا يذهب إلى أن الحيازة غير المشروعة لأرقام بطاقات الائتمان التي تتم عبر الإنترنت إنما هي على درجة كبيرة من الصعوبة، كعملية تقنية تحتاج إلى برمجة معقدة، ومن ثمّ تعد حركة الحيازة المادية لها أسهل بكثير من حيازتها عبر الإنترنت فإن حالات اختلاس هذه الأرقام عبر الإنترنت من الخطورة بمكان، وهو ما دفع المشرِّع الفيدرالي

(1) Dr. Andrzej Adamski (Nicholas Copernicus University, Toran, Poland). Crimes Related to the computer network, threats and opportunities: A criminological perspective OP-CIT, P.221.

الأمريكي إلى عَدِّها جريمةً وفق 18 (7) (1) (a) U.S.C. 1030 [1]. فقد حدث في عام 1996 أن تم اختراق حاسوب محمول LAPTOP يحتوي على 314,000 رقم لبطاقات ائتمان تخص أحد المكاتب التابعة لمؤسسة Visa Card INT في كاليفورنيا، وفي عام 1997 قام Carlos Sadalgo Jr. (37 عامًا) باستخدام حاسوب في جامعة سان فرانسيسكو واختلس أسماء مالكي وأرقام log-ons عدد 100,000 كارت ائتمان وكذلك بيانات أخرى من خلال اختراقه لمجموعة مزوِّدي خدمات إنترنت ISPs وقام بوضعها على أسطوانة مضغوطة CD ثم قام بتشفيرها وعرضها للبيع بمبلغ مائتين وخمسين ألف دولار، ولقد اكتشف عملاء المباحث الفيدرالية هذه الجريمة وحوكم سادالجو وعوقب بالسجن ثلاثين شهرًا[2].

**(ب) العدوان على التوقيع الإلكتروني**: يعد التوقيع Signature من الأهمية بمكان في سائر المعاملات، فهو التعبير الأمثل عن أصالة كل وثيقة، فأي مستند لا يتضمن توقيعًا لا يحمل بذاته إمكانية تفاعله مع القانون على أية شاكلة. والمحاكم لا تعتد بمجرد ورقة مكتوبة بخط اليد، إنما لكي تأخذ هذه الورقة حظها من الاعتبار القضائي فإنه يجب أن تكون ممهرة بتوقيع صاحبها Signatory

---

(1) Ibid.

(2) The CFAA makes it a crime for an unauthorized user to access a computer that is federally owned or is a «protected computer» for the purpose of 1) obtaining records from a bank, credit card issuer, or consumer reporting agency; 2) committing fraud or extortion; 3) transmitting destructive viruses or commands; 4) trafficking in stolen passwords; or 5) threatening to damage a computer system in order to extort money or other things of value. A «protected computer» is a computer 1) used exclusively by a financial institution or the United States Government; 2) used on a nonexclusive basis but where the conduct affects use by the financial institution or the government; or 3) used in interstate or foreign commerce or communication. This last element is intended to keep the federal government out of purely local computer crimes, but the multistate nature of Internet transmission suggests that almost any Internet activity will amount to «interstate commerce». see: James Garrity & Eoghan Casey. Internet Missue in the Workplace: A Lawyer's Primer, op. cit., at 14.

وباليد ذاتها التي كتبتها Manuseript signature، ومثل هذا الأمر تقليد إنساني معروف منذ القدم. ونتيجة لكثرة تداول التوقيع ولزومه في نسبة أي وثيقة إلى مصدرها الشخصي، فقد أهمل التشريع تعريف مصطلح التوقيع، إلا أنه نتيجة للتطورات الحادثة في القانون المعاصر على أثر خروج تكنولوجيا المعلومات إلى الوجود، وجدت الحاجة لتعريف محدد للتوقيع لكونه اصطبغ بالصفة الإلكترونية، حيث تستخدم الآلة في إعداده، وهو الأمر الذي ترتب عليه بالضرورة لزوم تحديد الوضعية التي يكون عليها مع لزوم شموله في الوضعية الإلكترونية بالحماية القانونية، سيّما في جوانبها الجنائية. ولقد قنَّن المشرِّع المقارن هذا الأمر للدلالة على أهمية التوقيع، فالمشرّع الأمريكي أوجب تعريفًا للتوقيع في مشروع قانون التجارة Uniform Commercial Code (UCC) حيث يُعَدُّ توقيعاً «كل رمز معتمد بقصد التعبير عن الأصالة».

والتوقيع الإلكتروني كأحد مظاهر التوقيع عامة كان ـ ولا يزال ـ أحد اهتمامات المشرع المقارن، ومن ذلك المشرع الأوروبي الذي أصدر توجيهًا في عام 1995 للشروع في تشكيل لجنة خبراء لكي تتولى وضع مشروع التوقيع الإلكتروني، وفي 16 الصيف/ يونيو/حزيران 1998 تقدمت اللجنة بمشروعها هذا مقترحة إصدار مجلس أوروبا توجيهًا بالخصوص، وفي 22 الطير/ إبريل/ نيسان 1999 وضع المشروع النهائي للتوجيه، ولقد قام البرلمان الأوروبي في 12 الكانون/ ديسمبر/ أيلول 1999 بإعداد نصوص التوجيه المذكور ليخرج علينا في ثوبه الأخير.

ولقد أصدر المشرّع الألماني قانون الإنترنت لسنة 1997 الذي يتضمن مجموعة نصوص حول الإنترنت المؤرخ في 22 يوليو/ تموز 1997 ومن بينها نصوص تتعلق بالتوقيع الإلكتروني.

كذلك اعترف المشرّع الفرنسي بالتوقيع الإلكتروني حيث تنص المادة (4 ـ 1316) من القانون المدني الفرنسي بعد تعديلها بالقانون رقم 230 ـ 2000 المؤرخ

13 مارس 2000 حيث تقرر بأن التوقيع الإلكتروني يعد وسيلة تعامل معترفًا بها، ومفترضًا صحته Pésumée إلى حين إثبات العكس. ولقد صدر المرسوم التنفيذي لهذا التعديل رقم 272 ـ 2001 المؤرخ 30/ 3/ 2001 بشأن تطبيق المادة (4 ـ 1316) من القانون المدني الفرنسي المتعلقة بالتوقيع الإلكتروني، حيث تضمن في المادة (1/ 1) تعريفًا أكثر تحديدًا للتوقيع الإلكتروني بأنه «معطيات ناتجة عن استعمال طريقة ردًا على شروط معرّفة في صدر الجملة المقررة في الفقرة الثانية من المادة (6 ـ 1316 ـ مدني)».

وفي إطار النظام القانوني الإنجليزي استطاع القضاء الإنجليزي في قضية Goodman V. J. Eban. Ltd تحديد الأصالة Authentication بالإضافة إلى مناهج التوقيع الإلكتروني. على إن الأمر لم يقف عند هذا الحد وإنما قامت إدارة التجارة والصناعة الإنجليزية Department of Trade and Industry في مارس 1999 بإصدار وثيقة استشارية Consultation Document بعنوان Building Confidence in Electronic Commerce تمّت هيكلتها على ضوء التوجيه الأوروبي المشار إليه أعلاه، وبناءً على هذه الوثيقة أصدر البرلمان الإنجليزي قانون الاتصالات للمملكة المتحدة المؤرخ 25/ 5/ 2000 The UK Electronic Communications Act الذي ينص في القسم (7) من على تعريف للتوقيع الإلكتروني[1].

وإمّا المشرّع البلجيكي فقد أصدر القانون المؤرخ 20 أكتوبر/ تشرين الأول 2000 الذي أضاف إلى القانون المدني البلجيكي المادة (2281) مقرراً الاعتراف

(1) Section 7(1) provides: In any legal proceedings:
(a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and
(b) the certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data, See: Chris Reed-What is a signature?, op. cit., at 15.

بالتوقيع الإلكتروني إلى جوار اعترافه بالتواقيع التي ترد عبر الفاكس والبريد الإلكتروني والبرقيات والتلكس وبأية وسيلة أخرى[1].

وإمّا المشرّع الأمريكي فقد اهتم اهتمامًا كبيرًا بموضوع التوقيع الإلكتروني لكونه أداة فعالة في حركة المعاملات المدنية والتجارية، وتحديدًا كان للمشرع الولائي الأمريكي الأسبقية في هذا الإطار، حيث أصدر مشرع ولاية Utah في عام 1995 أول تشريع للتوقيع الإلكتروني The digital signature act of 1995 الذي تم إلغاؤه وإعادة إصدار تشريع آخر في عام 1996، وكان من بين الأغراض التي سعى مشرّع ولاية يوتا الأمريكية بإصداره هذا التشريع، هو التخفيف من حدّة الاحتيال بالتزوير والنصب على التوقيعات ككل[2]. ثم تلا ذلك ولاية كاليفورنيا بقانون 5 سبتمبر 1995 الذي، بعد أن اعتبر التوقيع الإلكتروني في مرتبة التوقيع المادي، قام بتعريف التوقيع الإلكتروني في القسم (5 ـ 16) من كود الحكومة الولائية The Government Code بأنه «تحديد إلكتروني للهوية تم إعداده بوساطة الحاسوب ومعتمد من قبل مستخدمه لكي يكون له ذات القوة والأثر للتوقيع المادي أو اليدوي ولكن لا يشمل هذا التعريف إمكانيات التشفير»[3]. ولتتوالى بعد ذلك مظاهر الاهتمام بالتوقيع الإلكتروني من قبل المشرّع الوِلائي الأمريكي مثل تشريع ولاية أويامنغ Wvoming لعام 1995، ثم

---

(1) 20 OCTOBRE 2000, Loi introduisant l'utitisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire.
والمادة (2281 ـ مدني بلجيكي) هي المادة التي كان المشرع البلجيكي قد ألغاها بمقتضى القانون المؤرخ 15/ 12/ 1949. ولقد أعادها إلى الحياة في ثوب جديد بمقتضى القانون المؤرخ 2000 السالف.

(2) William E. Wyrough, JR & Ron Klein- The electronic signature act of 1996: Breaking down barriers to widespread electronic commerce in Florida, op. cit., at 429.

(3) «An electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual this definition does not include encryption. Further, signature», id at 431.

تشريع ولاية واشنطن Washington الصادر في 2 مارس/ آذار 1996 الذي اعتمد على تشريع ولاية يوتا، ومما تجدر الإشارة إليه أن تشريع واشنطن تقرر نفاذه مع الأول من شهر يناير/ كانون الثاني 1998.

ولكن ما هو التوقيع الإلكتروني تحديدًا، وما هو دوره في الحياة الاقتصادية الاجتماعية عبر الإنترنت، وما هي الاستفادة المرجوة منه إزاء تطلّب وجوده في حركة المعاملات، وفوق هذا كله هل تكفي النصوص الحالية لكي تتفاعل مع ظاهرة التوقيع الإلكتروني وبحيث تشمله بالحماية الكاملة؟

**1 ـ تعريف التوقيع الإلكتروني:** تعددت محاولات تعريف التوقيع الإلكتروني فاختلف الرأي بشأن تحديد تعريف موحَّد له، وإن كان يظل مظهر الاتفاق الوحيد ـ رغم الاختلاف ـ ممثلاً في ضرورة توافر طرف ثالث Third Party يطلق عليه سلطة تصديق التوقيع Certification Authority، والتي يتشابه عملها مع السلطة التي تكون للمصارف حال حجز مبالغ مالية لصالح المستفيد من إصدار الصكوك.

وفي إطار الاختلاف حول تعريف التوقيع الإلكتروني فإن هناك من يرى أن التوقيع الإلكتروني مجرد تسجيل إلكتروني E. Record، وهناك من جعل التوقيع الإلكتروني يرتقي إلى مستوى الهوية الإلكترونية E. Identity، وثالث استشعر مدى خطورة التوقيع الإلكتروني ليرى فيه صيغة تكنولوجية لها طابع ذاتي من حيث الأصالة E-signature is generic techneutral term لما له من القدرة على التداول العالمي بصرف النظر عن اعتبارات الحدود الدولية، بل إن هناك من يرى أن التوقيع الإلكتروني ليس سوى معالجة رياضية Mathematical Process تميز الوثائق الإلكترونية من حيث نَسَبها إلى أصحابها.

أما التوجيه الأوروبي المؤرخ 12/ 12/ 1999 المشار إليه فقد انطلق، في محاولة منه لاحتواء موضوع التوقيع الإلكتروني لكي يضع تعريفين له، أحدهما

موسّع والآخر مضيق، فالتعريف الموسع هو ما قررته المادة (2/ 1) من التوجيه بقولها «بيان في شكل إلكتروني يتفاعل بشكل منطقي مع البيانات الإلكترونية الأخرى وله طابع الأصالة كمنهج». وفي المادة (2/ 2) من التوجيه قرر المشرع الأوروبي «تعني عبارة توقيع إلكتروني متقدم، كل توقيع إلكتروني يتقابل مع أحد المتطلبات الآتية:

(أ) أن يكون مرتبطًاً كلّيةً بصاحبه.

(ب) أن يكون مؤهلاً للتعريف بصاحبه.

(ج) أن يكون متميزًا بما يسمح لصاحبه بالتحكم فيه.

(د) أن يكون مرتبطًا ببيانات ذات علاقة به بحيث يكون كل تغيير في البيانات المذكورة غير مقبول».

على أن التعريف الأمثل لدينا هو التعريف الذي يرى في التوقيع الإلكتروني أنه «مجموعة من الحروف أو الأشكال أو الرموز التي تبرز إلكترونيًا لها الأثر ذاته الذي يحدثه التوقيع المادي»[1]. فمثل هذا التعريف يضع فكرة التوقيع Signature في موضعها الصحيح ـ عندنا ـ من حيث أنها عبارة عن اسم شخص الموقع Signatory على الشيء المكتوب من قبله في نهاية ما هو مكتوب[2]، مع ما يشمل ذلك من عدم تحديد لما إذا كان الشخص طبيعيًا أم معنويًا، وهو التطور الذي قاده المشرع الأوروبي في هذا الإطار وفق ما قرره في توجيه 1999 في المادة (2/ 3) منه التي قررت أن عبارة الشخص كما قد يكون طبيعيًا فإنها أيضًا تشمل الأشخاص المعنوية في هذا الإطار.

(1) Thomas, Ruth, op. cit., at 4.

(2) William E. Wyrough JR & Ron Klein, The electronic signature act of 1996: breaking down barriers to widespread electronic commerce in Florida, op. cit., at 419.

كما يفيد هذا التعريف في تمييز التوقيع الإلكتروني عن التشفير والذي هو سلسلة من الخوارزميات التي ينبغي تبادلها مع الآخرين، في حين أن التوقيع الإلكتروني يخص الشخص ذاته فهو مالكه وليس للغير أن يتعامل به ولا يحدث بشأنه تبادل من أي نوع كما لا يعد انقسام التعامل فيه مبدأً يحكمه.

وللتوقيع الإلكتروني فائدة كبيرة عبر الإنترنت، وبصفة خاصة في نشاط التجارة الإلكترونية، فهو يخفف من حدة الاستخدام الورقي في الاتفاقات ثم إنه يسمح بقدر من المرونة في المعاملات أيضًا لكونه يجتاز مسألة الوقت فيختصر الزمن والمسافات أيضًا، إذ يكفي أن يضع الشخص توقيعه لكي تتم المعاملات دونما حاجة لانتقاله إلى مختلف الأماكن لكي يقوم بمعاملاته. ولعل أبسط الأمثلة التي تتعلق بالتوقيع الإلكتروني هي تلك التي يمكن اعتمادها في المصارف، حيث تتطلب المعاملات المصرفية وجود توقيع معترف به وبدونه لا تستقيم المعاملة تمامًا. ويفيد التوقيع الإلكتروني في كونه يسهل كثيرًا العمليات المصرفية.

على أن المشرّع المقارن لم ينته إلى اتفاق في مسألة تحديد الحماية القانونية والجنائية الواجبة للتوقيع الإلكتروني، فهناك اتجاه تشريعي يجعل التوقيع الإلكتروني في مستوى التشفير، وتالياً، ما ينطبق على التشفير من حماية قانونية ينطبق عل التوقيع الإلكتروني أيضًا، وذلك مثل تشريع كاليفورنيا. على أن هذا الاتجاه في الحقيقة لا يتناسب مع ما هو مقرر في التشريع ذاته من استواء التوقيع الإلكتروني بالتوقيع اليدوي من حيث القيمة القانونية والآثار التي تترتب على التوقيع. ولعل هذا الأمر هو الذي جعل المشرع الأوروبي يتجه مُتّجَهَ الاعتراف بعدم تمييز التوقيع الإلكتروني عن غيره كاليدوي مثلاً، مقررًا أن التوقيع كما قد يكون ماديًا أو يدويًا فإنه من الممكن أن يكون إلكترونيًا أيضًا. لأجل ذلك وضع المشرع الأوروبي تمييزًا في تعريف التوقيع الإلكتروني سواءٌ في صيغة عامة أو في صيغة مخصصة، فالصيغة العامة تفيد اعتراف المشرع

الأوروبي بالتوقيع الإلكتروني، في حين أن الصيغة المخصصة تفيد في تحديد مدى إمكانية امتداد الأثر القانوني للتوقيع حين يكون إلكترونيًا بحيث يصلح ـ إذا توافرت الخطوات اللازمة ـ أن يكون نافذًا أمام الجهات الرسمية كأن يكون دليل إثباتٍ أمام القضاء مثلاً، وهو الأمر الذي قررته المادة (2/5) من التوجيه الأوروبي.

**2 ـ مظاهر العدوان على التوقيع الإلكتروني**: كان توجه المشرع الأوروبي هو الانطلاق من اعتبار التوقيع الإلكتروني من البيانات الشخصية، لذلك لم يتوان عن التقرير بمسؤولية مزود خدمات توثيق التوقيع الإلكتروني prestataire de service de certification حال قيامه ببث التوقيع أو تسليمه لغير مالكه وهو ما قررته المادة (6) من التوجيه المذكور.

ولكي يتم العدوان على التوقيع الإلكتروني فإن ذلك يأخذ شكل العدوان على الأساليب الآمنة التي يتولاها طرف ثالث محايد Neutral Third Party، هو مقدم خدمات الإنترنت Online Service Provider OSPs، وذلك بالعدوان على وسائل التشفير الضرورية من مفتاح عام وآخر خاص. على إن الأمر قد يأخذ شكلاً آخر أكثر سهولة يتمثل في حالة تتبع التوقيع الإلكتروني لشخص ما، بما يستدعي الأمر هنا لزوم إحداث اختراق تام من خلال معرفة الخادم المشترك فيه هذا أو ذاك الشخص، ثم القيام بعد ذلك بالبحث فيه عن الهوية الإلكترونية IP الخاصة بذلك الشخص، حتى يتوصل إليها ثم بعد ذلك القيام باستنساخ التوقيع الإلكتروني خاص به.

**3 ـ نقد فكرة التوقيع الإلكتروني بحلول فكرة البصمة الإلكترونية**: إن الاتجاه المعاصر نحو إقرار واعتماد التوقيع الإلكتروني يعتبر من الموضوعات التي تُعدُّ محل نظر، سيما إزاء ارتباط فكرة التوقيع الإلكتروني بفكرة أخرى، لا تزال بعد في طور النمو، وهي فكرة التجارة الإلكترونية. فهذه الأخيرة تعد من

الموضوعات التي تعاني في القانون من مسألة تقويمه في الوقت الذي يعاني منها القانون من حيث اتصاله بها، وفيما إذا كان يعد العدوان على التوقيع الإلكتروني عدوانًا على الأموال أم على التشفير أم على الحق في الحياة الخاصة. . . الخ.

فإذا أضفنا إلى ذلك منطق الوسيط الإلكتروني الضامن لفكرة التوقيع الإلكتروني بمقتضى إقرار أو شهادة إلكترونية Le certifical Electronique التي تتعدد أنواعها عبر الإنترنت، والتي بمقتضاها يتم اعتماد التوقيع الإلكتروني فإن ذلك يقودنا بالضرورة إلى أن مسألة التوقيع الإلكتروني يمكن أن تُعد من المشكلات إزاء الدقة التي عليها مسألة التوقيع الإلكتروني هذه وما قد تثيره من مشكلات.

ولقد ازداد الأمر تطورًا حال بروز فكرة البصمة الإلكترونية التي تتفق في التصنيف مع فكرة وحدانية التوقيع في العالم المادي. إذ أن البصمة الإلكترونية تعبّر عن وحدانية التوقيع من حيث نسبته إلى شخص واحد فقط. وتتخذ البصمة الإلكترونية هنا الشكل ذاته التي هي عليه في العالم المادي، فقد تكون على هيئة وضع بصمة الإصبع أو العين أو الأسنان أو الصوت. . . الخ، إلا أنها في كل الأحوال ـ سواء في العالم المادي أو الافتراضي ـ فإنها تحتاج إلى الآلة لإقرارها. فمثلاً؛ من يريد الاتصال بحسابه المصرفي عبر الإنترنت، فإن الأمر لا يتطلب سوى وضع البصمة الإلكترونية على ماسح ضوئي خاص مرتبط بالحاسوب الذي يوصلها بحاسوب المصرف المذكور. . . وهكذا.

ومثل هذا الاتجاه الجديد يمكن أن يكون أكثر ثقة في التعاملات المالية لما تتمتع به بصمة الإنسان من ذاتية خاصة، حيث كل إنسان له بصمته الخاصة. والعدوان على البصمة كما يمثّل تزويرًا لتوقيع حيث تقوم البصمة مقام التوقيع إن لم تكن أقوى تأثيرًا منه، فإنه يمكن أن يكون الأمر كذلك عبر الإنترنت، حيث يقوم مقلد التوقيع بتزوير آليته.

## المبحث الثانـي:
## جريمة الاحتكار والاحتكار المضاد

الأصل دائمًا أن التجارة حرة لا يقيدها قانون ولا يؤثر فيها سوى حركة المستهلك. وهذا الأصل الاقتصادي لا يوجد سوى في خيال الاقتصاديين دائمًا، إلا أنه يمثل دائمًا نقطة الانطلاق الأولى في حركة تنظيم الاقتصاد، وبحيث يُعد دائمًا من الآمال التي أن تتحقق حتى في صيغة المدافعين عن مبدأ حرية التجارة. ذلك أنه طالما وجد القانون الاقتصادي حتى في صيغته العرفية، كان ذلك مؤشرًا على وجود قيد على المنافسة في إطار حركة السوق.

وحركة السوق تعني في إطار حرية التجارة والاقتصاد أن مبدأ المنافسة يمتد إلى القطاعات الاقتصادية كافة دون منازع بما في ذلك براءات الاختراع[1]. وإذا كان الاحتكار هو السيطرة على معدلات الاقتصاد في ظل نظم السوق التي تتبع اقتصاديات العرض والطلب، لكونه يتعارض مع مدلول الحرية الاقتصادية، وكذلك القوة الكامنة في التجارة من حيث كونها تعبر عن ذاتها، في منطق فرض هيمنة المنتج الأفضل لدى المستهلك النهائي، فإن عبارة الاحتكار المضاد تعد أخطر مجالاً في هذا الإطار، لكونها تمثل استنهاض الهمم لمواجهة العدوان على حركة اقتصاديات السوق الحرة بأقوى الأسلحة الاقتصادية على الإطلاق والممثلة تحديدًا في الترويج المجاني للسلع كنوع من الرد الاقتصادي على مساهمة حركة الإنتاج في الصراع الخفي الدائر في إطار اقتصاديات السوق الحرة. ويبرز مثل هذا الصراع، أكثر ما يبرز، في إطار صناعة الحاسوب والإنترنت.

---

(1) 35 USC Sec. 211 Relationship to antitrust laws: Nothing in this chapter shall be deemed to convey to any person immunity from civil or criminal liability, or to create any defenses to actions, under any antitrust law. SOURCE (Added Pub. L. 96-517, Sec. 6(a), Dec.12, 1980, 94 Stat, 3027). REFERENCES IN TEXT: The antitrust laws, referred to in text, are classified generally to chapter 1 (See. 1 et seq.) of Title 15, Commerce and Trade.

وإذا كان الاحتكار المضاد قد برز في أقوى صورة على يد الكبار في مجال الحاسوب، وتحديدًا في محاولات شركة مايكروسوفت للرد على القواصم التي تجتاح اقتصاديات إنتاجها من قبل العديد من الشركات مثل AOL (التي امتلكتها Time Warner في نهاية عام 2000) إلا إن ذلك لا يعني عِدادُ الاحتكار المضاد متميزًا عن الاحتكار في صورته التقليدية، بل هو في الحقيقة ضربٌ منه، إن لم يكن وليدُه، وهو في هذا المنحى تتوافر له مقومات عدم المشروعية.

على أنّ عدم المشروعية هنا لم ينتظمها قانون متفرد، وإنما ظلت القوانين المُجَرمة للاحتكار هي المسيطرة حتى على الاحتكار المضاد استنادًا إلى الطبيعة ذاتها التي عليها الاحتكار والاحتكار المضاد. والحقيقة، لقد كشفت قضية مايكروسوفت موضوع الاحتكار المضاد بشكل لم يسبق له مثيل، حيث أماطت هذه القضية اللثام عن علاقات السوق الخفية والصراع الباطني حول من يسود؟

وإذا كان مقصد المشرّع، في كل دولة تنتهج منهج الاقتصاد الحر، هو السعي إلى خلق المنافسة الكاملة كمقياس لحركة هذا الاقتصاد، فإن لعبة الاحتكار المضاد يمكن أن تكون على درجة عالية من الخطورة، وسلاح فتاك تضر في النهاية بالمستهلك النهائي الذي يستفيد من صراع المنافسة دائمًا.

والقاعدة التي تحكم الاحتكار هي البحث دائمًا عن مجال متكافئ للمنافسة في حركة التجارة وبحيث ينشأ الاحتكار دائمًا حين يظهر عدوان على المنافسة. وتقتضي المنافسةُ أن تتصف بالمشروعية دائمًا، فإذا وجد ما يفيد المنافسة هنا فإن ذلك مؤشر على دخولها في حركة الاحتكار المضاد.

## أولاً: الاحتكار والاحتكار المضاد عبر الإنترنت

لقد برز العديدُ من المشكلات فيما يتعلق بالاحتكار والاحتكار المضاد والإنترنت، ولقد برز هذا الأمر تحديدًا في مشكلات أخذت الطابع البسيط ثم

تطورت لتأخذ حظها الكبير من الرؤية القانونية. وإذا كان المشرع المقارن يتجه إلى حصر الإنترنت في المجال القانوني، في محاولة منه لتقييد السلوك السلبي عبر الإنترنت، فإن هذا التقييد يُعدّ احتكارًا قانونيًا في الحقيقة، وليس احتكارًا عدوانيًا أو إجراميًا. ومثل هذا الأمر يجعل منطق حصر المشرع المقارن لمجموعة من الأعمال، وكذلك تحصين بعض المؤسسات من قاعدة الاحتكار، إنما هو من الأمور اللازمة في هذا الشأن، فالمشرّع الأمريكي يرى في اللجنة الفيدرالية للاتصالات FCC مؤسسة مشروعة، ولا يمكن تشبيهها بمزود خدمات أو غيره من مؤسسات الإنترنت، وكذلك فَعلَ المشرّع الفرنسي في اللجنة الوطنية للاتصالات CNIL. فمثل هذه المؤسسات لا تعد محتكرة لحركة الاتصالات في مجال تكنولوجيا المعلومات، وإنما هي في الحقيقة ذات أغراض محددة، وأهم هذه الأغراض تسيير العالم الافتراضي تقنيًا دونما سيطرة عليه في هذا الشأن، ويبرز ذلك في الأثر الكبير الذي صاحب تعديلات قانون الاتصالات الأمريكي لسنة 1934 بالقانون الصادر في 1996، حيث توسعت تلك التعديلات في منح صلاحيات مزودي الخدمات عبر الإنترنت.

وإذا كان الاحتكار كمصطلح يأخذ في مجراه التحكم في حركة العرض والطلب في نظرية السوق، فإن الاحتكار المضاد يعني بالضرورة العدوان على المنافسة Anti Competation أثناء احتدامها في السوق من حيث الواقع العملي، بحيث يكون الأمر قد برز على أثر صراعات تنافسية حول مُنتجَ، أو البحث في القدرة على الاستحواذ عليه فيما يتعلق بحركة التوزيع أو الاستهلاك، وفي هذه الحالة الأخيرة لا يكون المستهلك حرًا في اختياراته وإنما يلجأ إلى جهة واحدة تكون قد سيطرت على سوق التوزيع. لذلك فإن الاحتكار المضاد له المضار ذاتها التي تكون للاحتكار فيما خلا أن المنتج يكون فعلاً في السوق وينتج عن سلسلة من السلوك غير المشروع بقصد السيطرة عليه. ويمكن إعطاء مثالٍ حيّ عن الاحتكار المضاد في عام 1999، عند قيام شركة Intel صاحبة أشهر

معالجات مصغّرة Microprocessors في العالم بالرد اقتصاديًا على المنافسة بالإبقاء على منطق حجب التقنية والتأثير في الأسعار، كنوع من الثأر والانتقام من عملائها ممن هم حاصلون على امتيازات براءات اختراع Patents لديها[1] كونهم قاموا بممارسة ضغوط اقتصادية عليها حين رفضوا القيام باستصدار تراخيص منها، على أثر اشتعال سوق المعالجات العالمية.

## ثانيًا: الجريمة في التشريع المقارن

إن موضوع الاحتكار والاحتكار المضاد أو العدوان على المنافسة هو من الموضوعات التي أخذت حظها في إطار المفاهيم الاقتصادية للقانون. فقد نبتت الفكرة في القانون المقارن في مجال التفسير الاقتصادي تحديدًا، وما توصل إليه القانون العام الإنجليزي English Common Law، حيث استمد مفهوم الاحتكار Monopoly ومكافحة الاحتكار Anti-Monopoly منه دعمًا للمنافسة Competition على أسس مشروعة. ولقد قامت الولايات، صاحبة الاختصاص الأصيل في القانون العام الأمريكي، بتقوية نظم المنافسة فيها على أسس مكافحة العدوان على المنافسة المشروعة، ومنهج التحالفات الكبرى، وذلك وفق مفاهيم القانون العام فيها والمستمدة مبادئه من النظام الأنجلوفوني. ومن ذلك كسر حِدّة الاحتكار لدى كبار المحتكرين في العصر حديث، من أمثال Rockefeller صاحب مؤسسة Stanford Oil of NJ التي امتلكت (90٪) من مصافي النفط، كما سيطر على حركة نقل النفط العالمي مع نهاية القرن التاسع عشر.

ولقد كان ذلك دافعًا إلى نشاط حركة المشرّع الأمريكي في اتجاه

(1) William J. Bear & David A. Balto-Antitrust Enforcement & High Teconoloy Markets, April 30, 1999, Telecommunications & Technology Law Review Vol. 73/1999, P.7, available online in March 2000 at http://www.mttlr.org/volfive/balto.html.

المحافظة على منهج القانون العام في تنمية المنافسة المشروعة، مع ترك منهج مكافحة العدوان على المنافسة المشروعة للتشريع، فكان أن وافق المشرّع الفيدرالي في عام 1890 على مشروع قانون كان قد تقدم به عضو الكونجرس تشيرمان، ولقد أطلق على هذا التشريع قانون تشيرمان The Sherman Act نسبة إليه، وهو القانون الذي تمّ ضمّه إلى القسم الخامس عشر (15 US Code 1) من التقنين الأمريكي. ويعد قانون تشيرمان عصب سياسة مكافحة الاحتكار في الولايات المتحدة الأمريكية، وهو القانون الذي لحقه قانون كلايتون (15 US Code 12) The Clayton Act وقانون لجنة التجارة الفيدرالية The Federal Trade Commission Act, 15 U.S.C. 41 اللذيْن صدرا في عام 1914. ويتضمن قانون تشيرمان ركيزتين: إذ بمقتضى القسم الأول منه تم إعلان عدم مشروعية العقود والاتفاقات التي تقيد من التجارة مثل التعاقدات التي تؤدي إلى الاحتكار أو الدمج Combination المؤدي إلى قيام الاحتكار أو التآمر Conspiracy بين الأشخاص الاعتباريين بقصد الاحتكار والتحكم في الأسعار، في حين يحظر القسم الثاني الاحتكار والشروع في الاحتكار.

أما قانون كلايتون ـ المعدِّل لقانون تشيرمان السالف ـ والذي تم تعديله لاحقًا بمقتضى قانون روبنسون باتمان في عام 1939، وكذلك قانون سيلير كافوفر في عام 1950، يتعامل مع أربعة أشكال من الأنشطة ذات العلاقة بالمال والأعمال وهي: تمييز الأسعار (Sec.2) price discrimination والاتفاقات والتنظيمات المقيدة (Sec.3) exclusive dealing and tying arrangements والاندماج (Sec.7) mergers ومركزية الإدارة وتشابك العمل الإداري Interlocking directorates (Sec. 8).

أما قانون لجنة التجارة الفيدرالية FTC فقد تضمن ما يفيد مكافحة الوسائل غير العادلة في المنافسة في التجارة ما بين الولايات، والأعمال المضللة في الأنشطة التجارية حيث عُدّت غير مشروعة.

## ثالثًا: الاحتكار عبر الإنترنت

مما سلف يمكن القول إجمالاً أن الاحتكار يطلق عليه لدى الدول التي تعتنق مفهومه أنه تعبير عن كفاح القانون الجنائي ضد نظرية المؤامرات الاقتصادية Conspiracy Theories. على أن السؤال يظل هنا مرتبطًا في هذه الدراسة بمعرفة مدى إمكانية حضور الاحتكار عبر الإنترنت، وفيما إذا كان لمبدأ المنافسة المشروعة وجود في العالم الافتراضي. ومثل هذا التساؤل أجاب الفقه عليه بالإيجاب مقررًا إن الاحتكار له وجود عبر الإنترنت، ويبرز ذلك تحديدًا في برمجيات الحاسوب وبرمجيات الإنترنت والتي تُلحق بالضرورة بالحاسوب لكي يمكن تنفيذها عبر الإنترنت، سيما فيما يتعلق بتطبيق قواعد قررها القضاء المقارن، مثل قاعدة اليد المغلولة The Hands-off Rule.

إننا إذا استثنينا لجنة الاتصالات الفيدرالية ودورها في عملية الاتصالات في العالم الرقمي فإنه يمكن القول أن الاحتكار عبر الإنترنت برز في المنافسة غير المشروعة التي قادتها مجموعة شركات كبرى في مجال تكنولوجيا المعلومات وعلى رأسها مايكروسوفت الأمريكية. حيث يمكن القول إن الاحتكار عبر الإنترنت نشط في اتجاه حرب المتصفحات Browser Wars، تلك الحرب الشرسة التي بدأت في ولاية نيويورك ثم امتدت إلى العالم أجمع، وشغلت الرأي العام العالمي، سيما وإنها تمس كبرى شركات البرمجيات العالمية والتي تملك زمام الأمور في نظم التشغيل الأكثر شعبية، والتي على رأسها برامج التشغيل، والبيئة التكنولوجية الأكثر شعبية، برمجية النوافذ Windows. فهي القضية التي جعلت المسؤول الأول في الشركة Bill Gates يصرخ في أحد مقالاته بعبارته الشهيرة قائلاً (أو مستجديًا) Why they're doing this?.

ولكن ما هي الأسس التي استند إليها القضاء الأمريكي في إدانة شركة مايكروسوفت وإصدار ذلك الحكم القاسي بتفكيكها إلى شركتين منفصلتين. ثم

ما هي العوامل التي جعلت المحكمة الاستئنافية تنتهي إلى نقض حكم أول درجة المذكور؟ وهنا نجد إنه من اللازم أن نتعرض لهذه القضية لكونها تمثل أولى القضايا في حرب المتصفحات عبر الإنترنت.

## رابعًا: قضية مايكروسوفت[1]

بشكلٍ موجز، بدأت وقائع هذه القضية عندما نشطت مايكروسوفت في تحديث متصفحها بعد خروج نظام النوافذ 95، سيما وإن شركة AOL America On Line كانت قد بدأت نسبيًا في الترويج لمتصفحها الشهير Netscape NN Navigator الذي كان يعد الأكثر رواجًا آنذاك، وهو الأمر الذي استشعرت معه مايكروسوفت خطورة موقفها، حيث إن البيئة التي يعمل فيها NN هي بيئة النوافذ. ونتيجة لصراع خفي بين شركات أخرى (مثل Intel صاحبة المعالج الشهير المسمى باسمها وSun Microsystems صاحبة برمجية JAVA وهي شركات كانت على علاقات تعاقدية مع مايكروسوفت، قامت الأخيرة باتخاذ خطوات جدية وسريعة وعملية باتجاه تطوير متصفح الإنترنت الذي تملكه Internet Explorer (والملحق ببرمجية النوافذ)، وبصدور النسخة المطورة من برمجية النوافذ 98 أعلنت مايكروسوفت أن إصدار النسخة المطورة من متصفحها Explorer سوف يكون مجانيًا، كونه من ملحقات برمجية النوافذ أصالةً، وهو الأمر الذي جعل شركة AOL ورئيسها آنذاك Stave Case يشتاط غضبًا، يسانده في ذلك مجموعة من الشركات كانت تأمل أن ترى مايكروسوفت تتهاوى نتيجة لرؤيتها الخاصة حول تنمية فكرة تكنولوجيا المعلومات، وعلى النحو الذي يجعلها أكثر شعبية مما هي عليه، والتي أفصحت عنها منذ خلافها الأول مع شركة IBM في ثمانينات القرن المنصرم.

---

(1) تولى الادعاء في هذه القضية السيد Joel Klein وكيل النائب العام في جرائم الاحتكار، وأما القاضي فقد كان السيد Thomas Penfield Jackson المسمّى قاضيًا في عهد الرئيس ريغان.

كان ذلك ملخص الأحداث التي دفعت إلى اتهام مايكروسوفت بالاحتكار، وعندما رفعت الدعوى إلى القضاء ـ عن طريق ادعاء قضاء نيويورك ـ ليقول كلمته فيها في 19/ 10/ 1998، كان محك الصراع القضائي لكي يمكن التوصل إلى الصيغة التي يتم بمقتضاها تحديد الطابع الاحتكاري لـ. . مايكروسوفت هو الإجابة على الأسئلة الثلاثة التالية:

- النظر فيما إذا كانت مايكروسوفت تملك قوى احتكارية Monopoly Power في سوق نظم تشغيل الحاسوب الشخصي PCOSs؟
- النظر فيما إذا كانت مايكروسوفت دخلت في علاقات قوية مع غيرها لحماية هيمنة نظام التشغيل Windows من المنافسة، باستخدام نهج عملي منظم؟
- النظر فيما إذا كان نشاط مايكروسوفت قد أساء إلى الابتكار وكذلك إلى المستهلكين؟

(أ) **القوة الاحتكارية لمايكروسوفت**: وهذه تمثل النقطة الأولى المشار إليها أعلاه. ولقد لوحظ فيما يتعلق بالقوة الاحتكارية لشركة مايكروسوفت تلك القدرات الكبيرة لديها في السيطرة على المعالجات المتوافقة Processes Compatible لشركة Intel، وهي المعالجات التي يمكنها جعل الحاسوب يعمل بكفاءة لا تصل إلى المستوى الذي تحققه حواسيب متكاملة مثل حواسيب IBM وCompaq مثلاً، إلا أن هذه المعالجات جعلت سوق الحاسوب يتسع للقاعدة الشعبية حول العالم. ونتيجة لوجود هذا المعالج في السوق التجارية فإن مايكروسوفت سيطرت على (90٪) من نظم التشغيل في العالم[1].

(1) Stephen Tolbert, op.cit at 3.

(ب) **سلوكيات مايكروسوفت**: بادرت مايكروسوفت بانتهاج مسلك الإعداد لحرب طويلة الأمد ضد مؤسسة AOL مالكة المتصفح NN آنذاك، حيث قامت بإنفاق الوقت والجهد والمال على تطوير متصفحها IE، ثم بعد ذلك قامت بترويجه مجانًا، مما جعل ذلك السلوك يبدو مقيدًا لتكنولوجيا المعلومات. كما صدر عن مايكروسوفت سلوك يتضمن بحدّ ذاته وسيلة ضغط على بعض الشركات، مثل تهديدها الكتابي لشركات مثل شركة Compaq بإلغاء ترخيص Intel إذا لم يتم تحميل متصفح مايكروسوفت المتطور IE على نظام التشغيل Windows في حواسيبها. كذلك عندما رفضت شركة IBM الشهيرة عرض مايكروسوفت بتطوير نظم التشغيل Windows قامت الأخيرة بمعاقبتها برفع أسعار الترخيص المذكور. كما سارت مايكروسوفت على المنوال ذاته بالنسبة للعديد من الشركات التي تعمل في مجال الحوسبة مثل Real Network, Sun Microsystems, Appel.

(ج) **الإساءة إلى المستهلك**: يُعدّ ما قامت به مايكروسوفت مظهرًا من مظاهر مكافحة المنافسة Anti-Competitive كونها قيدت المستهلك النهائي، وهو المستخدم لنظام التشغيل، وحقه في الاختيار[1]، سيما وإن المستهلك المذكور يرتبط بنظام التشغيل هذا طالما أنه يستخدم الحاسوب برمجةً وعملاً وإبحارًا عبر الإنترنت أيضًا، بحيث لن يكون له الحق في وجود اختيارات تسمح بالمنافسة كحد أقصى أو أنها تسمح بعدم الاحتكار في الحد الأدنى.

وحسبما سلف فإن مايكروسوفت بدأت في مسلك الاحتكار من حيث أنها

(1) Stephen Tolbert, op.cit at 2.

قامت بشكل غير مشروع بربط متصفحها IE في نظام تشغيلها Windows 98 وذلك يشكل انتهاكًا للقسم الأول من قانون تشيرمان، كما أنها قامت بالسيطرة على سوق متصفحات الإنترنت Web Browser Market بالمخالفة للقسم الثاني من قانون تشيرمان. حيث إن مايكروسوفت بذلك حاولت السيطرة في سلوكياتها هذه على سوق تكنولوجيات البرمجة بربطها بنظام تشغيلها، بالشكل الذي يجعله مصدر الحياة الكامل لكل برمجية يمكن أن يقوم الغير بإعدادها، وهو ما جعل القضاء يرى في ذلك انتهاكًا للمعايير التي تحكم الاستهلاك والمستهلك عن طريق تحديد الأسعار Price Fixing [(1)]، مما يجعل مايكروسوفت تقع تحت طائلة القسم الثاني من قانون تشيرمان.

لذلك كله اتجه قضاء أول درجة[(2)] إلى الإقرار بإدانة مايكروسوفت، وذلك بفرض عقوبة علاجية عليها، حيث استلزم في هذه العقوبة فرض منهج المنافسة عليها بقوة القانون، وذلك بفصل خط إنتاج البرمجيات في شركة مايكروسوفت عن خط إنتاج نظام التشغيل فيها بما يجعل الانفصال انفصالاً قائمًا بين عمل الحاسوب وبين عمل الإنترنت، وإنشاء ثلاث شركات لبرمجية النوافذ كل منها مستقلة عن الأخرى استقلالاً كليًا في إطار الملكية الفكرية، وبحيث يكون لها أيضًا استقلالية الالتزام. على أن الانتصار الكبير الذي حققته الحكومة الأمريكية ضد مايكروسوفت لم يستمر طويلاً، فقد نقضت محكمة الاستئناف حكم أول درجة في 28/ 6/ 2001 (محكمة الاستئناف لمقاطعة كولومبيا)، لأسباب تتعلق بعدم ثبوت الاحتكار بحيث بدا الأمر لمحكمة الاستئناف هنا كما لو كانت المنافسة ليست للسيطرة على سوق المتصفحات، وإنما احتدم الجدل

(1) Price Fixing among competitors is a horizontal restraint and a per se violation of the Sherman Act. See: Shawn W. Potter, op. cit at 20.

(2) US v. Microsoft Corp, 56 F. 3d 1448 (D. C. Cir. 1995) («Microsoft 1»). See also: United States v. Microsoft Corp., 147 F. 3d 935 (D.C. Cir. 1998) («Microsoft II»).

حول بيئة النوافذ التي تحتاج إلى مجهودات شركات أخرى في الوقت الذي تملك مايكروسوفت هذه البيئة في تشغيل الحواسيب، وبما يجعل الغير في حاجة إلى مايكروسوفت، ومثل هذا الأمر يخضع لإرادة الشركات الأخرى وليس لإرادة مايكروسوفت التي تملك مثل هذا المنتج الناجح شعبيًا. وكان من ضمن هذه الأسباب ما يتعلق بصلاحية قاضي المحكمة لكونه خالف نظام القضاء المقرر في القسم 28 U.S.C. Sec. 455(a)، بقيامه بالتصريح للصحافة أثناء نظره للقضية[1].

## المبحث الثالث:
## الجرائم التي تمس الأخلاق

إن التعرض لجرائم الأخلاق عبر الإنترنت ليس بالموضوع السهل، إذ يجد الباحث ذاته في إطار هذه النوعية من الجرائم عرضةً لبحث الاختلاف الاجتماعي على المستوى الأخلاقي والقائم بين الحضارات، بل وحتى بين المجتمعات في الدولة الواحدة، فيبرز له بصورة منطقية أن هناك اختلافًا في طبائع المجتمع ومستويات النظرة الفردية الاجتماعية إلى الأمور لكونها ترتبط بمفهوم المدنيات المعاصرة. وارتباطها كذلك بمنطق أو نهج التعامل مع الإنسان في المجتمع. فما يكون يُعدّ انحلالاً أخلاقيًا في حضارة أو دولة أو مجتمع معين قد لا يكون كذلك في نهج دولة أخرى، وقد يختلف في نهج دولة ثالثة. . . وهكذا.

لذلك فإنه يلاحظ أنه وإن كان ليس هناك بُدّ من التطرق إلى هذه النوعية من الجرائم حين تتم عبر الإنترنت، فإن ذلك لا يعني سوى التطرق إلى الحلول التي طرحها المشرِّع لهذه النوعية من الجرائم، من حيث كونها خلقت مشكلة

(1) US. V. Microsoft Co., App. Colombia No. 00-5212, 00-5213 (No. 98cv01233), June 28, 2001.

ذات شأن كبير، على الرغم من حركة الإباحة الأخلاقية التي تجتاح بعض المجتمعات غير الإسلامية.

وجرائم الأخلاق، وفقًا للتصنيف المصلحي في قانون العقوبات، هي تلك النوعية من الجرائم التي تتضمن العدوان على القيم الأخلاقية المتعارف عليها في النظم الاجتماعية الاقتصادية.

ويُعدّ العدوان في جرائم الأخلاق من ضمن أشكال العدوان على القيم الإنسانية الاجتماعية، مع ما يُصاحب هذا الأمر من تشدد في الطابع الحضاري لتلك القيم، وهو التشدّد المستوحى مما تعارف عليه الناس وارتضوه قاعدةً أخلاقيةً، وهو أمر يفترض تباين الحضارات والثقافات في المستوى الأخلاقي، إذ من الممكن أن يكون ما هو غير أخلاقي في حضارة معينة معاصرة، مُعَدٌّ أخلاقيًا في حضارة أخرى معاصرة أيضًا. وإذا كان ذلك صحيحًا إلا أن هذا لا يعني عدم وجود حد أدنى لقواعد أخلاقية يمكن أن تكون أساسًا لقانون عقوبات عالمي مستوحى من الأخلاقيات الذاتية للشعوب.

ولقد أولى المشرع المقارن اهتمامًا ملحوظًا بالجرائم الأخلاقية، وفقًا لما تمليه عليه حضارته، كما أسلفنا، وذلك يعني تحديدًا أن الاختلاف الحضاري لا يؤدي إلى نزع الأخلاق من الحضارات، وإنما تختلف النظرة إليها من حضارة إلى أخرى فحسب. فالمشرع الليبي رصد الجرائم الأخلاقية في الباب الثالث من الكتاب الثالث من قانون العقوبات لسنة 1953 في المواد من (407) إلى (424)، ثم إنه يرتب آثارًا على ارتكاب مثل هذه النوعية من الجرائم في التشريعات الأخرى، لكون العامل الأخلاقي في ليبيا مستمدًا من الحضارة الإسلامية الرشيدة ومنطق التقاليد التي تأسس عليها هذا المجتمع في إحداث البنية الأخلاقية هناك. والأمر ذاته ينطبق على التشريع المصري وكذلك التشريع الصادر في الدول العربية والإسلامية، في حين انه في التشريع الصادر في الدول غير العربية وغير الإسلامية، فإنّ الحال أنّ المشرع يستمدّ المعيار الأخلاقي من

المنطق الاجتماعي الاقتصادي لديه، إلا أن ذلك لا يعني انعدام وجود العامل الأخلاقي، بل إنه كثيرًا ما يلاحظ قوة العامل الأخلاقي، وعلى أساسه تقوم فكرة الحقوق المدنية هناك.

## العلنية والعرض للجمهور والمصطلح الأخلاقي عبر الإنترنت

إن العدوان على الأخلاق عبر الإنترنت يُعد، في الحقيقة، من المشاكل التي جعلت الاصطدام قويًا بين المشرّع والقضاء في القانون المقارن، ولقد احتلت مشكلة الأخلاق عبر الإنترنت حيزًا كبيرًا في بحوث الفقه المقارن، في عملية صراع كبيرة ما بين حرية التعبير واحترام أخلاقيات الشعوب. إذ إن المشرّع المقارن لا يتوانى عن سن التشريعات التي تحمي القواعد الأخلاقية، إلا أن القضاء المقارن يقوم بإلغاء هذه التشريعات سعيًا وراء حماية حرية التعبير، كإحدى الحريات التي تتفوق على الأخلاق. ومع ذلك فإن المشرع، كردة فعل، يقوم مرة أخرى بإعادة سن التشريعات بغرض حماية الأخلاق، بحيث مثلت القاعدة الأخلاقية على هذا النحو تحديًا بين المشرّع والقضاء في القانون المقارن.

وفي هذا الفرع سوف نتعرض لثلاثة موضوعات دقيقة في مضمونها حين الارتباط بالإنترنت، وهي موضوعات العلنية والعرض للجمهور والمصطلح الأخلاقي عبر الإنترنت، لكونها أثارت جدلاً في القضاء المقارن.

**أولاً: شرط العلنية**: العلنية Publication وصف لحالة حدث أو عمل أو نشاط يباشره الشخص في حدود القانون. فليست العلنية قيمة في ذاتها وإنما تبرز تلك القيمة في مدى تأثيرها في الحدث بحيث تجعله ينتقل بمقتضى هذا التأثير إلى الجمهور، وبحيث يترتب على وصفه بالعلنية نتائج يعترف بها القانون ويرتب عليها آثاره.

وقد ينص المشرّع في تشريعه العقابي على نص عام يحتوي منطق العلنية

ينطبق على سائر الجرائم، مثلما هو الحال فيما هو مقرر في المادة (16/ 1 ـ عقوبات ليبي) التي تنص على أنه تُعدّ الجريمة مرتكبة علنية إذا كان ارتكابها: (أ) بطريق الصحافة أو غيرها من وسائل الدعاية والنشر، (ب) في محل عام أو مفتوح أو معروض للجمهور وبحضور عدة أشخاص، (ج) في اجتماع لا يُعدّ خاصًا نظرًا للمكان الذي انعقد فيه أو لعدد الحاضرين أو للغرض الذي عقد من أجله»، ويُعدّ مثل هذا النص قاعدة عامة تضمنها القسم العام من قانون العقوبات بحيث يتم تفسير كلمة العلنية كلما وردت في النصوص على ضوئها. ولا يعني رصد قاعدة عامة تؤدي دورها كتعريف أو تحديد امتناع المشرع عن رصد معنى مخصّص للعلنية، بل يمكنه القيام بذلك كما هو الشأن في المواد (284 ـ 286 ـ عقوبات ليبي)[1].

ولعل المُثار في مقصود العلنية، المدى الذي عرض له المشرّع الجنائي هنا، وتالياً أنواعها المشار إليها، لاسيما فيما يتعلق بالفرق بين المحل العام أو المفتوح أو المعروض للجمهور، وبين عبارة الاجتماع الذي لا يعد خاصًا نظرًا للمكان الذي انعقد فيه أو لعدد الحاضرين أو للغرض الذي عقد من أجله. وهذا يقود بالضرورة إلى القول بأن كل اجتماع خاص، بالنظر إلى المكان الذي أعِدّ فيه أو لعدد الحاضرين أو للغرض الذي أعد من أجله، يجعل العلنية منتفية عن

(1) تنص المادة (284 ـ عقوبات ليبي) على أنه «يعاقب بالحبس مدة لا تزيد على سنة وبغرامة تتراوح بين عشرين ومائة دينار أو بإحدى هاتين العقوبتين كل من أذاع بطريق الصحافة أو بأي طريق آخر من طرق العلانية بيانًا عن قضية جنائية نظرت سرًا أو أذاع محتويات وثائق أو أوراق تتعلق بتحقيق في قضية يجب أن تبقى سرية قانونًا. ولا يطبق هذا الحكم على الوثائق وحيثيات التحقيق التي أدلى بها فيما بعد في مناقشة علنية وبوجه عام لا يطبق على سائر أوراق الإجراءات الجنائية القضائية بعد انقضاء ثلاثين سنة على الفصل فيها أو قبل ذلك إذا أذن وزير العدل بالنشر صراحة. ولا يعاقب في الأحوال المنصوص عليها في الفقرة الأولى من هذه المادة على مجرد الإعلان عن القضية ولا نشر الحكم فيها فقط». وتنص المادة (286 ـ عقوبات ليبي) على أنه «يعاقب بالعقوبات المذكورة في المادة السابقة كل من نشر بأي طريقة من طرق العلانية المداولات السرية بالمحاكم أو نشر بغير أمانة وبسوء قصد ما جرى في الجلسات العلنية بالمحاكم».

الواقعة، كما هو الشأن في الاجتماع الذي يعقد في منزل ما للعائلة إذا حدث وتبادل بعضهم ضدّ بعض عبارات قذف وسب، ففي هذه الحالة لا تتوافر العلنية. ومن ثم فإن وجود شبكة داخلية بين أفراد العائلة ليست مرتبطة بالإنترنت وإنما تظل بين أفراد العائلة الواحدة في نطاق مكاني موزع وليس محدداً فإنه لا تتوافر فيه صفة العلنية حال وجود واقعة سَبّ أو قذف، حتى مع إمكانية حدوث الاختراق هنا لكون المُختَرِق مرتكبًا لجريمة انتهاء حق الخصوصية ولو كانت الصفة التي تواجد بها هي الحضور مصادفة.

وإذا تأملنا التمييز بين المحلّ العام أو المفتوح أو المعروض للجمهور وبين عبارة الاجتماع الذي لا يُعدّ خاصًا نظرًا للمكان الذي انعقد فيه أو لعدد الحاضرين أو للغرض الذي عقد من أجله، فإن القضاء المقارن كان قد تعرض له في التمييز المحض بين عبارتي To the public وIn the Public، حال التعرض لقانون حق المؤلف، بحيث اعتبرت محكمة الاستئناف الفيدرالية لـ. كيبك/ كندا بأن عبارة To the public أعم من عبارة In the public، فهذه الأخيرة يتناسب مدلولها مع منطق الاجتماع الذي لا يعد خاصًا نظرًا للمكان الذي انعقد فيه أو لعدد الحاضرين أو للغرض الذي عقد من أجله، في حين أن العبارة الأولى تندمج في فكرة المحلّ العام أو المفتوح أو المعروض للجمهور، وهو الأمر الذي يترتب عليه القول أنه في الاتصال المباشر فإن المجموعات الإخبارية Newsgroups تُعد محلاً عامًا أو مفتوحًا أو معروضًا للجمهور حال وجود إمكانية لأي شخص أن يلج إليها دونما شروط خاصة، في حين تكون هذه المجموعة الإخبارية اجتماعًا لا يُعد خاصاً إذا كان مكان انعقاده على الإنترنت محددًا بموقع معين (إذ يستطيع أي شخص أن يستدعيه)، إلا أنه في الوقت ذاته يحتاج إلى تحديد هويةٍ وكلمة مرورٍ لكي يمكن للشخص الولوج إلى موقع المجموعة الإخبارية، وفي هذه الحالة فإن الأمر يصير إلى العلنية أيضًا، أما إذا كانت المجموعة الإخبارية مرتبطة بشبكة خاصة، وهذا الأمر كثير الحدوث، كما لو

كان هناك شركة أو مؤسسة تملك شبكة خاصة بها فإن تداول الأحاديث بنظام المجموعات الإخبارية والاجتماعات المغلقة عبر الشبكة المذكورة لا تتوافر فيه العلنية، لكون الولوج إليها من قبل الغير، إنما يعد ولوجًا غير مشروع طالما لم تتوافر فيه المشروعية الكافية لذلك(1).

وقد لا يرى المشرّع ضرورةً للنصّ على قاعدة عامة تتضمن تفسيرًا للعلنية، مكتفيًا بتحديد مصطلح العلنية في نصوص خاصة معتمدًا في تحديد نطاق تفسيرها على ما يقرره القضاء في هذا الشأن، مثلما هو حال المشرّع المصري في المادة (171 ـ عقوبات مصري) التي تنص على أنه «كل من أغرى واحدًا أو أكثر بارتكاب جناية أو جنحة بقولٍ أو صياحٍ جهر به علنًا أو بفعل أو إيماءٍ صدرٍ منه علنًا أو بكتابة أو رسوم أو صور شمسية أو رموز أو أية طريقة أخرى من طرق التمثيل جعلها علنيةً أو بأية وسيلة أخرى من وسائل العلنية، يعد شريكًا في وقوع تلك الجناية أو الجنحة بالفعل. أما إذا ترتب على الإغراء مجرد الشروع في الجريمة ليطبق القاضي الأحكام القانونية في العقاب على الشروع. ويعتبر القول أو الصياح علنًا إذا حصل الجهر به أو ترديده بإحدى الوسائل الميكانيكية في محفل عام أو طريق عام أو أي مكان آخر مطروق أو إذا حصل الجهر به أو ترديده بحيث يستطيع سماعه من كان في مثل ذلك الطريق أو المكان أو إذا أذيع بطريقة اللاسلكي أو بأية طريقة أخرى. ويكون الفعل أو الإيماء علنيًا إذا وقع في محفل عام أو طريق عام أو في أي مكان آخر مطروق، أو إذا وقع بحيث يستطيع رؤيته من كان في مثل ذلك الطريق أو المكان، وتعتبر الكتابة والرسوم والصور الشمسية والرموز وغيرها من طرق التمثيل العلنية إذا وزعت بغير تمييز على عدد من الناس أو إذا عرضت بحيث يستطيع أن يراها من يكون

(1) Commission du droit d'auteur - Canada, Public Performance of Musical Works 1996, 1997, 1998 - Public Performance of Musical Works - Copyright Act, Section 67.2, October 27, 1999, P.29.

في الطريق العام أو أي مكان مطروق أو إذا بيعت أو عرضت للبيع في أي مكان».

وفي النصّ الأخير يلاحظ أن المشرّع المصري ساوى في التجريم بين القول العلني والإيماءة العلنية والفعل العلني والكتابة العلنية. . .الخ. فالقول هو الصوت ويمكن أن يكون مصدره مباشرًا كما هو الشأن في جريمة السبّ، وقد يكون غير مباشر، كما هو الشأن في التشهير عبر الصحف أو في الإذاعة. والإيماءة هي الإشارة، والفعل هو الحركة العضوية العلنية ما دامت تتضمن تعبيرًا ما، والكتابة هي التدوين بلغة مفهومة قصد التعبير عن فكرة أو موضوع ويلحق بها الرسوم والصور الشمسية والتصوير الخيالي، كالكاريكاتير والتصوير المرئي والرمزي[1]. وقد تكون الكتابة بطريق النشر وقد تكون مراسلة خاصة، إلا أنه نظرًا لطبيعة الوسيلة التي تم بها الإرسال تكون قد استقرت في إطار العلنية، كما هو الشأن حين إرسال فاكس أو برقية. . .الخ، بحيث يكون قد اطلع عدد من الناس عليها قبل وصولها إلى المجني عليه. على أن السؤال هنا يتعلق بالبحث عن مدى أهمية تطلب العلنية في جرائم الأخلاق للقول بإمكانية قيام التجريم في مثل هذه الأحوال. ذلك أن بعض جرائم الأخلاق تتم في السر، بل وإنها تشترط السرية كواقع، وما دور القانون هنا سوى البحث في مدى وقوعها لكي يرتب عليها نتائجه.

والواقع أن العلنية ذات شأن في بعض جرائم الأخلاق وليس كلها مثلما هو الحال في الفعل الفاضح العلني، والبث الفاضح، أو الفاحش العلني والتعرض لأنثى (420 مكرر ـ عقوبات ليبي) التي تنص على أنه «يعاقب بالحبس مدة لا تقل شهر ولا تزيد عن ستة أشهر كل من تعرض لأنثى على وجه يخدش حياءها بالقول أو الفعل أو الإشارة في طريق عام أو مكان مطروق. وكل من

(1) د. جميل عبد الباقي الصغير: الإنترنت والقانون الجنائي، الجوانب الموضوعية، المرجع السابق، ص68.

حرض المارة على الفسق بإشارات أو أقوال أو أفعال. وتكون العقوبة الحبس مدة لا تقل عن شهرين ولا تزيد عن سنة إذا عاد الجاني إلى ارتكاب جريمة من نفس نوع الجرائم المشار إليها في الفقرة السالفة خلال سنة من تاريخ الحكم عليه، ولا يجوز في هذه الحالة الأمر بإيقاف تنفيذ العقوبة المحكوم بها».

ولما كانت الإنترنت من وسائل العلنية ـ بطبيعتها ـ فإن ذلك يقودنا إلى ضرورة بحث هذه المسألة، إلا أننا سوف نتجه إلى رصد البحث في العلنية عبر الإنترنت في كل حالة على حدة، سعيًا وراء التقرير بأن العلنية عبر الإنترنت ينبغي تطلبها لكون الأفعال التي تعد جريمة عبر الإنترنت كثيرة ومتنوعة، بما يعني أن العلنية متطلَّبة حال تطلُّب المشرّع لها وبحيث لا تكون العلنية شرطًا عامًا ينبغي توافره كلما كان هناك جريمة عبر الإنترنت.

ويلزم ذلك بالطبع التعرض للمصطلحات القانونية التي يستخدمها المشرع المقارن لتحديد الفعل اللا أخلاقي عبر الإنترنت، ثم تطرق إلى التشريع المقارن ودوره في رصد الإجرام الأخلاقي عبر الإنترنت وذلك كتمهيد إلى تحديد الجرائم الأخلاقية في هذا المطلب.

## مسألة العرض للجمهور

ورد مصطلح العرض للجمهور في القانون الليبي في معرض المادة (16/ 1 ـ ب ـ عقوبات) حيث قرر المشرع إمكانية عداد الجريمة مركبة علانية إذا ارتكبت في محل معروض للجمهور، في حين قرر المشرع المصري منطق العرض للجمهور في الباب الرابع عشر من قانون العقوبات، في المواد (171) وما بعدها، لا سيّما المادة (178، ثالثًا/ 2 ـ عقوبات مصري) التي رددت مصطلح «وكل من أعلن عنه أو عرضه على أنظار الجمهور»، ففي الحالتين تتوافر العلنية المتطلبة في الجرائم التي يتطلب فيها المشرع لزوم العلنية.

وفيما يتعلق بتحديد الجريمة الأخلاقية التي يمكن أن ترتكب علنًا عبر

الإنترنت، يمكن القول بأن المصطلح المستخدم في التشريع المصري يمكن أن يحقق نوعًا من التوافق مع شبكة المعلومات الدولية/ الإنترنت، بحيث أن ما هو موضوع أو موجود على هذه الشبكة من مواد، أياً كانت يمكن القول بأنه يتم عرضه من قبل شخص ما على أعضاء (جمهور) الإنترنت، في حين لا يمكن أن تكون الإنترنت محلاً معروضًا للجمهور، لأن الإنترنت ليست محلاً، حيث أن مقصود المحل في النص الليبي هو النطاق الجغرافي الذي يجمل على مفهوم الحيز المكاني المادي، في حين أن العرض على الجمهور وفقًا للنص المصري لا يستدعي أن يكون المحل الذي تم العرض فيه محلاً معروضًا للجمهور في معنى الحيز، وإنما كل ما تطلبه المشرع هنا هو العرض على الجمهور بأية وسيلة كانت، سواء كانت في العالم المادي أو في غيره. ولما كانت الإنترنت وسيلة اتصالات جماهيرية فإن المفترض الصحيح، وفقًا للقانون المصري دون الليبي هنا، إنه بمجرد وضع المادة المجرمة على شبكة المعلومات الدولية/ الإنترنت تكون قد تم الإعلان عنها أو عرضها على الجمهور، دون حاجة لإقامة الدليل على أن جمهورًا قد اطلع على المادة الإجرامية من عدمه.

وعندما أن نصّ المادة (178، ثالثًا/ 2 ـ عقوبات مصري)[1] يمكن أن تجد لها مكانًا من التطبيق في جرائم الإنترنت، دون نص المادة (16/ 1 ـ ب ـ عقوبات ليبي). فمثلاً من يسمح للغير بوضع أية مقالة أو أية كتابة من أي نوع

(1) تنص المادة (178، ثالثًا ـ عقوبات مصري) على أنه «يعاقب بالحبس كل من صنع أو حاز بقصد الاتجار أو التوزيع أو الإيجار أو اللصق أو العرض صورًا من شأنها الإساءة في سمعة البلاد، سواء أكان ذلك بمخالفة الحقيقة أو بإعطاء وصف غير صحيح أو بإبراز مظاهر غير لائقة أو بأية طريق أخرى. ويعاقب بهذه العقوبة كل من استورد أو صدر أو نقل عمدًا بنفسه أو بغيره شيئًا مما تقدم للغرض المذكور، وكل من أعلن عنه أو عرضه على أنظار الجمهور أو باعه أو أجره أو عرضه للبيع أو الإيجار ولو في غير علانية، وكل من قدمه علانية بطريقة مباشرة أو غير مباشرة ولو بالمجان وفي صورة من الصور وكل من وزعه أو سلمه للتوزيع بأية وسيلة. فإذا ارتكبت الجرائم المنصوص عليها في هذه المادة عن طريق الصحف سرى في شأنها حكم المادة السابقة.

عبر إحدى صفحات موقعه على شبكة المعلومات الدولية/ الإنترنت، فإنه يكون قد قبل أن يوضع أي شيء مكتوب على موقعه، ويكون صاحب الموقع هنا هو من يقوم بالإعلان عنها أو بعرضها على الجمهور، وفي هذه الحالة يسري عليه نص المادة (178، ثالثًا/ 2- عقوبات مصري) في من يعيب في حق ممثل دولة أجنبية معتمد في مصر بسبب أمور تتعلق بوظيفته، وفي المادة (182- عقوبات مصري) عن طرق كتابة إعلان أو مقال، ولو لم يكن صحفيًا وإنما يتضمن تشهيرًا، ويقوم بوضعه على موقع عبر الإنترنت مسموح فيه بهذا الوضع، لا يكون قد قام هو بالعرض وإنما يُعاقب مقترف لجريمة تشهير هنا، كذلك من يرتكب جريمة المادة (102/ 1- عقوبات مصري) بإذاعة إشاعة من شأنها تكدير الرأي العام وإلقاء الرعب بين الناس وإلحاق الضرر بالمصلحة العامة إذا أنشأ موقعًا على الإنترنت تضمن مثل هذه الإشاعة[1]، فضلاً عن ذلك يعاقب مالك الموقع حتى ولو لم يكن هو كاتب عبارات التشهير، ذلك إن مالك أو صاحب الموقع عبر الإنترنت هو الشخص الذي تولى العرض على الجمهور، فما يعاقب عليه القانون وفق هذه المادة هو مجرد العرض على أنظار الجمهور دون أن يكون متطلبًا أن يكون العارض هو ممن صدرت عنه مواد العيب.

وعندما يمكن القول بصلاحية هذه المادة للانطباق على الجرائم المرتكبة عبر مواقع تسمح باستخدام صفحات فيها للتعبير عن فكرة أو طرح موضوع من قبل الجمهور، ففي هذه الحالة يظل صاحب الموقع عرضة للمسؤولية الجنائية والقانونية عما قد يرتكب من جرائم عبر موقعه إذا لم يتخذ الاحتياطات لمنع مثل هذا العيب وكذلك التدابير الكافية لتصحيح مثل هذه الوضعية وبما ينبئ عن حسن نيته في هذا الإطار.

والسبب الذي يجعلنا نتجه إلى اعتناق هذا الذي سلف، هو أنه ما دام قد

---

(1) انظر محكمة جنح النزهة بمصر ـ الحكم في القضية رقم 457 لسنة 2002 الموافق 11/ 4/ 2002 جنح أمن الدولة طوارئ.

تسيّد الاتجاهُ القانوني المقامَ في تنظيم الإنترنت، فإنه لا يمكن أن يتم القبول بالخروج عن النظام الاجتماعي الاقتصادي أو النظام العام عبر الإنترنت، ومن ثم يسري على الإنترنت مقومات النظم الاجتماعية الاقتصادية ذاتها. ولا يمكن الاحتجاج هنا بعدم معرفة أو علم صاحب الموقع الذي يتضمن صفحة إعلانية مجانية بالمادة المنشورة، حال كونها مجرمة، ففي مثل هذه الأحوال يلزم التقرير بأن مجرد فتح الصفحة للجمهور لكتابة ما يشاء فإن مسؤوليته تكون قائمة لقبوله المسبق بهذا الإعلان أو العرض على الجمهور للمادة أيًا كانت. ويلاحظ هنا أن القبول بالإعلان أو بالعرض على الجمهور ليس مفترضًا بل أنه واقعي، وهو قائم في الواقع لكون الارتضاء بالإعلان مسبقًا يمكن أن يكون له تشابه مع حقيقة من يملك لوحة إعلانات مجانية معروضة على أنظار الجمهور يضع فيها من يشاء أية مواد معيبة في حق الغير، ففي هذه الحالة يكون صاحب اللوحة المذكورة هو من يقوم بالإعلان عن مادة ليست ملكًا له وإنما للغير، ومن ثم تقوم المسؤولية في حقه حتى ولو لم يكن صاحب المادة معروفًا أو كان مُمهِرًا كتابته باسم مستعار. بخاصة إذا كان صاحب الموقع المذكور يستغل الصفحات، التي بعدها الغير مجانًا، في نشر إعلانات.

## المصطلحات غير الأخلاقية التي يتداولها القانون الجنائي

نتيجة للفارق الحضاري في قوانين الأخلاق والناتج الحضاري الاجتماعي في هذا الشأن، فإن كثيرًا من التشريعات يميز فيها بين الفعل غير الأخلاقي Indecency وبين الفحش Obscenity والدعارة المصورة Pornography. ويترتب على هذه المفارقة نتائج شتى في التشريع المقارن، إلا أنها في الواقع الاجتماعي من حيث الاختلاف الحضاري، فإن وقع أو تأثير كل من هذه المصطلحات له أساس يرتبط بمدى الحرية الأخلاقية التي يمنحها المجتمع لأفراده، وإلى أي مدى يمكن أن تصل، بل إنه في بعض التشريعات المقارنة تمكّن المشرّع من إلغاء التشريعات التي تعاقب على الزنا الإرادي، مثلما هو

الحال في التشريعين الفرنسي والأمريكي، تاركًا مثل هذا الفعل منتظمًا في إطار ردة الفعل الاجتماعي وأحيانًا الديني.

ولعل من موجبات التذكير حين التعرض للتعدد الاصطلاحي في القانون المقارن (بل في إطار كل قانون أيضًا) إن المشرع لم يتعرض على الإطلاق لتحديد معنى موحد لمصطلحات الأخلاق الواردة في القانون الجنائي، ففي القانون الأمريكي قرر القضاء إن مصطلح غير أخلاقي Indecent مصطلح غامض Vague [1]. كذلك لم يرد فيه على الإطلاق أي تعريف لمصطلح الدعارة المصورة في القانون ذاته[2]، ويبرز ذلك واضحًا في التوسع الكبير الذي تسير عليه المحكمة الفيدرالية العليا الأمريكية في تحديد مصطلح الفحش Obsecenity، حيث يمكن لهذا المصطلح استيعاب المصطلحات الواردة في القسم 1461 وما بعدها من الباب 18 وكذلك القسم 223 من الباب47 من التقنين الأمريكي[3]، وهي مصطلحات الفاحش Obscene والفسق Lewd والشهوانية Lascivious وكذلك البذاءة Filthy [4]، سيما تلك النصوص التي تتضمن جرائم غير أخلاقية باستخدام الإنترنت والحاسوب[5].

ولقد كان القضاء الأمريكي واضحًا في تحديد إمكانية العقاب، بمقتضى القسم (1461)، إذا تم استخدام مصطلحات الفحش بطريق المراسلة، سواء

(1) Reno V. ACLU No. 96-511 (U.S. Jun 26, 1997), US sup Court.

(2) Herb Lin, PHD hlin@nas.edu, Michele Kipke, PHD mkipke@nas.edu mailto:mkipke@nas.edu - Tools and strategies for protecting kids from pornography and their applicability to other inappropriate internet content, P.6, Computer science and telecommunicatins board on children, youth, and families, the national academies, available online in dec. 2000 at:
http://www.nationalacademies.org.

(3) 18 U.S.C. Sec. 1461 to 1469; 47 U.S.C. Sec. 223.

(4) Roth V. usa, Supp. 354 U.S. 476 (1957).

(5) 18 U.S.C. Sec. 1462, 1465.

تضمنت هذه المراسلة إرسال كتاب أو بانفليت Pamphlet أو مطبوع Printing أو أية وسيلة إعلانية Publication تحتوي على هيئة لا أخلاقية[1].

ولقد تأكد هذا التفسير في عام 1962[2] حيث قررت المحكمة العليا الأمريكية له أنه في إطار الاستخدام العام لمصطلحات الفحش فإنها تتخذ أشكالاً مختلفة من المعاني[3]. إلا أن المحكمة العليا عادت في عام (1976) لتضع منطقًا جديدًا لمصطلح الفحش، حيث رفضت مطلقًا التحديد القديم المشمول بالغموض Vagueness Challenge حين تفسير القسم 1461 المشار إليه، وذهبت إلى أن هذه المصطلحات الواردة في القسم المذكور إنما هي مجموعة مصطلحات محددة بشكل ظاهر في وصف السلوك الجنسي Hard Core الذي يعطى كمثال في أثناء الكلام[4]. كما أن القانون الليبي لم يحدد ما هو أخلاقي أو داعر أو فاحش من حيث التعريف، على الرغم من إن القضاء يقوم بدور كبير في رصد القيم الاجتماعية ومدى تفاعلها مع النصوص القانونية في هذا الشأن.

ومثل هذا الأمر يجعل بحث نقاط الاتصال، ومعايير تمييز ما هو أخلاقي وما هو غير ذلك، وكذلك تصنيف الأفعال غير الأخلاقية، من الأمور التي ترتبط بالفهم الاجتماعي الذي يأخذ طابع التعدد حتى في البيئة الواحدة.

لأجل ذلك نجد أن المحكمة العليا الأمريكية استندت حين نظرها قضية Reno v. ACLU، فيما يتعلق بقانون آداب الاتصالات 1996، إلى معيار قاضي المحكمة الابتدائية التي أصدرت الحكم المطعون فيه، وهو القاضي Sloviter، حيث استعان هذا القاضي بمعيار ورد في قضية أخرى هي قضية Sable Communication v. FCC حيث قررت المحكمة في هذه القضية الأخيرة أن

---

(1) Roth v. USA, op. cit.

(2) Manual Enterprises, Inc v. Day, Supp. 370 (1962).

(3) Id «while in common usage the words have different shades of meaning, the statute since its inception has been aimed at obnoxiosly debasing portrayals of sex».

(4) Haming v. USA Supp. 418 U.S. 87 (1974).

العبارات الجنسية تُعد غير أخلاقية، ولكنها على العكس من العبارات الفاحشة فهي مشمولة بحماية الدستور الأمريكي في التعديل الأول منه.

ولكل ما تقدم فإننا نقول إنه إذا كان هناك مجال لتحديد المعيار الأخلاقي عبر الإنترنت، فإن محاولات القضاء المقارن في هذا الإطار إنما تأتي تعبيرًا عن المنطق، الاجتماعي السائد، وبحيث يجب الاستعانة هنا فيما هو متعارف عليه في المجتمع، ولكن يظل هنا التذكير بأن المنطق الاجتماعي Community Standards له أهمية كبيرة في تحديد عناصر الجريمة الأخلاقية بحيث يتم الاستناد إليه كأساس للبحث في الوقائع.

وربما يعطي مثال استخدام اللهجات العامية العربية وغير العربية ـ والتي تختلف من محيط اجتماعي إلى آخر، وقد يكون هذا الاختلاف بادياً للعيان حتى في إطار الدولة الواحدة ـ إشارة واضحة المعالم إلى إمكانية التفاعل مع العامل الأخلاقي، بحيث يمكن حين استخدام هذه اللهجة أو تلك أن تفهم على نحو خاطئ من قبل بعض الذين ينتمون إلى فئة اجتماعية أو جهة جغرافية قد تكون في الدولة ذاتها، مثل هذا الأمر يجعل مذهب القضاء الأمريكي له قبول في المنطق والقانون على السواء إذا أدركنا أن المشكلة التي تواجه المشرع والقضاء والفقه هنا يتم التعبير عنها في استحياء شديد سعيًا وراء الإجابة على سؤال مقتضاه «أية معايير اجتماعية هي تلك التي يتم تطبيقها»؟

ولقد أخذ القضاء الأمريكي في الإجابة على هذا التساؤل منحى جديدًا بعض الشيء فيما يتعلق بتطبيق المعايير الاجتماعية على جرائم الأخلاق التي ترتكب عبر الإنترنت، حيث أخذ في الاعتبار المعايير الأخلاقية السائدة في المكان المرسل إليه المواد غير الأخلاقية، ثم تطور الأمر أكثر بحيث قرر القضاء الأمريكي الاستناد إلى معايير ثابتة غير مختلف عليها اجتماعيًا كما هو الشأن في دعارة الأطفال مثلاً، بحيث لا يلتفت القضاء في هذه الحالة إلى بث المعايير الاجتماعية.

ومن الأهمية بمكان التطرّق إلى نقطة تفاعل الإنترنت مع الجانب الأخلاقي في الإنسان، فقد أثيرت هذه المسألة بشكل جعل التفاعل التشريعي لازمًا معها، حتى إن استشعار مدى أهمية التدخل التشريعي يوحي بأن هذه مشكلة لم يكن لها وجود في عالمنا المادي، وإن أول بروز لها كان في العالم الافتراضي/ الإنترنت.

ولقد كان المشرع الأوروبي نشطاً في نهاية القرن العشرين في مجال حماية الأخلاق عبر الإنترنت، سيما بعد قيامه بإصدار التوجيه رقم 95/46/EC المؤرخ 24/ 10/ 1995 المتعلق بالتداول الحر للبيانات عبر الإنترنت، فقد أصدر مجلس أوروبا الكتاب الأخضر بشأن حماية القاصرين الذي نشر في شهر أكتوبر 1996.

أما في القانون الإنجليزي فقط أمكن للقضاء هنا التوصل مبكرًا إلى طرح موضوع الفحش Obscene، حيث تعرضت محكمة استئناف إنجلترا عام 1997 لمسألة تحديد تفسير لمصطلح الفحش. ولقد وجدت المحكمة في معرض تفسيرها للمصطلحات الواردة في قانون حماية الأطفال لسنة 1978 وقانون علنية الدعارة لسنة 1959، بأنهما لا يلتقيان مع فكرة التراسل الإلكتروني للبيانات The electronic transmission، حيث كانت هناك مشكلتان تعترضان القضاء الإنجليزي في التوصل إلى تفسير محدّد لهذا المصطلح، وتالياً تفسير القانونين بما يتفق وتكنولوجيا المعلومات، الأولى وتتعلق بمحتوى النسخة المرئية The Visual Image الموضوعة Stored في ذاكرة الحاسوب، حيث أنها تعد نسخة من الصورة A copy of a Photograph كما هي مقررة في التشيع، حيث أن المحكمة انتهت في شأنها إلى أنها موضوعة في القرص الصلب، وهي عبارة عن صورة مرئية تم مسحها Scanned [1] من ذلك القرص الصلب لكي يتم تحويلها Transmission إلى قرص صلب في حاسوب آخر، وهي على الشاكلة ذاتها دون

(1) Scanning is accomplished by dividing a picture up into little tiny elements called pixels. Sec: David J. Loundy-E-Law S. op. cit at 28.

تغيير في هيئتها وبالتالي تنتقل إلى الحاسوب الآخر كما هي A copy of a Photograph لأغراض تطبيق قانون عام 1978. أما المشكلة الثانية فتتعلق بمدى إمكانية وجود تساوٍ Tantamount بين وضع الصور المذكورة في القرص الصلب لحاسوب ما، وبين حركة توزيع هذه الصور. بحيث تختلف نية وضع هذه الصور عن تلك المتطلبة لتوزيعها.

ولقد انتهت محكمة استئناف إنجلترا في حكمها بالإدانة إلى التقرير بأن مجرد وضع شخص ما لصور دعارة في القرص الصلب لحاسوب ما، وبين حركة توزيع هذه الصور، بحيث تختلف نية وضع هذه الصور عن تلك المتطلبة لتوزيعها.

ولقد انتهت محكمة استئناف إنجلترا في حكمها بالإدانة إلى التقرير بأن مجرد وضع شخص ما لصور دعارة في القرص الصلب لحاسوبه فإن ذلك يعني أن هذا الوضع كان بقصد أن يطلع عليها هو، فإذا قام هذا الشخص بفتح حاسوبه للغير فإن ذلك يقاس على حالة فتح مكتبة للإطلاع على محتوياتها، إذ سمح صاحب المكتبة بمنح نسخة من المفتاح للغير هنا[1].

وبتعديل كل من هذه التشريعات، بسبب تكنولوجيا المعلومات وتأثيرها على القانون المعاصر، بمقتضى قانون العدالة الجنائية والنظام العام لسنة 1994[2]، وضع المشرع مصطلحًا جديدًا هو Pseudo - Photograph المقرر في القسم (7.7) من قانون 1978، والذي يشير إلى الاعتراف بالمنظر/ الصورة Image، التي تم إعدادها عبر برمجيات الحاسوب التصويرية أو بوسيلة أخرى، كصورة Photograph [3].

إن الاستفهام الذي يمكن أن يثار هنا يتعلق بالبحث فيما إذا كان هناك تنوع

---

(1) Id.

(2) The criminal justice & Public Order act.

(3) Id.

في الجريمة الأخلاقية عبر الإنترنت. وهذا الأمر سوف نتولى العرض له في الفقرة التالية توصلاً إلى تحديد تقسيم مصلحي لهذه الجريمة.

إن أشكال الجرائم الأخلاقية عبر الإنترنت تتميز بخصيصة ثابتة تتمتع بها كلها، وهذه الخصيصة تتمثل في أن أنماط الجريمة الأخلاقية كافة عبر الإنترنت تشترك في كونها لا تتجاوز الطابع المرئي/ المقروء، وغير المجسم، بحيث لا تسقط في مرحلة الحس الجسدي أو المادي، إلا إذا تحولت هذه النوعية من الجرائم إلى الاتصال المادي العادي بما يستدعي ذلك الخروج من العالم الافتراضي On line والعودة إلى العالم المادي Off Line، لذلك فمن غير المتصور أن تكون جرائم الأخلاق عبر الإنترنت جرائم مادية. وعليه فكل ما يمكن استحداثه من تقسيمات لنوعية جرائم الأخلاق عبر الإنترنت يجعلها كلها تشترك في طريقة تكوينها اللامادي أو المعنوي. ويظل السؤال هنا كامنًا في مدى إمكانية تعامل النصوص الجنائية الحالية مع جرائم الأخلاق عبر الإنترنت، وما إذا كانت هناك حاجة لتطوير النصوص المتعلقة بالجرائم الأخلاقية لكي تتوافق مع طبيعتها الرسمية وبحيث لا تكون الإنترنت وسيلة لارتكاب جرائم أخلاقية ويظل مرتكبها في مأمن من العقاب.

ولكي يتم لنا صناعة هذا الطلب فإننا هنا سوف نقوم بإحداث تقسيم مصلحي يتفق مع الإنترنت من ناحية، ومن ناحية أخرى يعبر في الوقت ذاته عن إمكانية احتوائه لمثل هذه النوعية من الجرائم دون عناء الاستعانة بطريقة التقسيم التقليدية التي درج عليها الفقه حين تعرضه لهذه النوعية من الجرائم، وذلك بسبب عدم إمكانية ارتكاب جميع الجرائم الأخلاقية عبر الإنترنت.

إذن، في هذا المطلب سوف نتناول بالبحث جرائم الأخلاق الممكن ارتكابها عبر الإنترنت، فليس كل الأفعال الأخلاقية المقررة في قانون العقوبات يمكن ارتكابها عبر الإنترنت، ومثل هذا الأمر يقودنا إلى الإقرار بجزئية أو نسبية جرائم الأخلاق عبر الإنترنت. على أن هذه النسبية أثارت موضوع جرائم

الأخلاق عبر الإنترنت بشكل جدلي، فمثلت تلك الجرائم أعتى أشكال الجرائم لما تتمتع به الإنترنت من تحرر رقابي غير مسبوق.

وعليه، يمكن استحداث تقسيم لجرائم الأخلاق عبر الإنترنت بحيث نتعرض لفكرة الترويج السمعي المرئي الفاضح، ثم نتطرق إلى موضوع جرائم البث العلني الأخلاقية من حيث جرائم النشر والقذف والسب والتشهير، ثم ننتقل إلى جريمة المطاردة الأخلاقية التي لها أساس في التجريم غير الأخلاقي وانتقل بعد ذلك إلى التجريم الأخلاقي.

## المبحث الرابع:
## جريمة الترويج السماعي والمرئي الفاضح

### أولاً: مصطلح الترويج عبر الإنترنت

إن مصطلح الترويج له صبغة العمومية لكونه قد يكون بمقابل أو بغير مقابل، فهو كمصطلح أعمّ من مجرد البث. والترويج وإن كان مجانياً لا يعني إمكانية قيام الغير بملك منتجات ما، وإنما كل ما في الأمر أن انعدام المقابل إنما يعني انفتاح أو إمكانية وجود قَدْر من الحرية في استعمال الشيء أو المنتج.

ويمكن أن يتسع الترويج عبر الإنترنت كذلك ليشمل المحادثة الشفهية بأية وسيلة كانت كالتي تتم عبر الفيديو الرقمي أو البث الحي له بطريق الإنترنت أو بطريق الدوائر المغلقة كعرض الشهادة في المحاكم أو تناول موضوعات عامة عن بعد. ولعل أخطر مظاهر الترويج السمعي المرئي هو أن يلحقه صفة الفضح فيما يصطلح عليه باللغة الإنجليزية بعبارة Cyber Audio-Visual Indecent، فمثلاً القيام بالاتصال بالغير باستخدام الإمكانيات السمعية المرئية عبر الإنترنت، مع القيام بحركات أو إيماءات فاضحة، من الأمور التي يمكن أن تشكل جريمة ما هنا، ويزداد الأمر صعوبة حالة وجود نوع من التداول لمثل هذه الحركات

السمعية المرئية الفاضحة، من خلال تسجيلها والقيام بتداولها عبر الإنترنت، والمشرّع المقارن يهتم في صيغة تقليدية بمثل هذه الجرائم، من خلال التعامل بالفيديو في العالم المادي كما هو الشأن فيما هو مقرر في المادة (178/ 1 ـ عقوبات مصري)[1] التي امتدت إلى المعاقبة على حيازة شرائط فيديو مخلة بالآداب، سواء كانت هذه الحيازة بقصد الاتجار أو العرض بمقابل أو بدون مقابل[2]. وهو الأمر المعاقب عليه في القانون الأمريكي بمقتضى القسم (18 US Code Sec 2252) التي تعاقب على الاتجار والنقل Transporting والحيازة Possession لبرمجيات حاسوب تتضمن دعارة أطفال[3].

على أنه نتيجة لتنوع أساليب الترويج السمعي المرئي الفاضح عبر الإنترنت، ما بين بث صور فاضحة ووثائق مكتوبة إلى عرض مرئي مختلف الأحجام، إلى ملفات صوتية تروي قصصًا جنسية. والغالب الأعم من هذه الأنماط والأنواع يتم بثه عبر شبكة المعلومات الدولية www. إلا أن البعض الآخر يتم ترويجه أيضًا عبر الشبكة القديمة كالمجموعات الإخبارية Use net Groups. فقد قام المشرع المقارن بتطوير آلية تشريعه لكي تتواءم مع هذا الأمر

---

(1) تنص المادة (178/ 1 ـ عقوبات مصري) على أنه «يعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تقل عن خمسة آلاف جنيه ولا تزيد على عشرة آلاف جنيه أو بإحدى هاتين العقوبتين كل من صنع أو حاز بقصد الاتجار أو التوزيع أو الإيجار أو اللصق أو العرض مطبوعات أو مخطوطات أو رسومات أو إعلانات أو صورًا محفورة أو منقوشة أو رسومات يدوية أو فوتوغرافية أو إشارات رمزية أو غير ذلك من الأشياء أو الصور عامة إذا كانت منافية للآداب العامة.

(2) طعن جنائي مصري رقم 3116 لسنة 55ق جلسة 28/ 10/ 1987 المكتب الفني لمحكمة النقض المصرية السنة 38 صفحة رقم 878 ـ ولقد أشارت المادة (1/ 2) من قانون المطبوعات المصري رقم 20 لسنة 1936 (الوقائع المصرية العدد 23 في 2/ 3/ 1936 ـ موسوعات التشريعات العربية) إلى أنه يقصد بالتداول بين المطبوعات أو عرضها للبيع أو توزيعها أو إلصاقها بالجدران أو عرضها في شبابيك المحلات أو أي عمل آخر يجعلها بوجه من الوجوه في متناول عدد من الأشخاص. انظر: د. جميل الصغير، الأحكام الموضوعية، السابق، ص89.

(3) USA v.Miller, App 11th Cir No.98-8228, Feb. 4-1999, Available online in March 1999 at: http://www.lp.findlaw.com/scripts/getcase.pl?navby=search&case.../988228man.htm

كما هو الشأن في التشريع الإنجليزي الذي وسع من فكرة النشر العلني Publication لمواد فاحشة Obscene matter المقررة في قانون الفحش العلني لسنة 1959، بمقتضى قانون العدالة الجنائية والنظام العام لسنة 1994، لكي تشمل التداول بالحاسوب Computer Transmission لصور Images ونصوص Text [(1)].

ومن الأشكال ذات الخطورة الخاصة في الترويج السمعي المرئي الفاضح عبر الإنترنت ما تتمتع به هذه الأخيرة من طبيعة اتصالية، إذ يمكن أن يقوم الأشخاص في هذا المجال بتبادل الأحاديث الجنسية، وهو ما يطلق عليه عبارة Cybersex، حيث يكون الحديث بين أشخاص لا يعرف بعضهم البعض الآخر، وبحيث يختلف الحال هنا عن الاتصال الذي يجريه الشخص بعاهرات بطريق الهاتف كنوع من الخدمات الإباحية التي تقدم في العالم الغربي في هذا المجال. حيث يمكن لأي كان أن يقوم بتنظيم نشاط إباحي عبر الإنترنت، كترتيب مواعيد جنسية وكذلك اختيار الهدف الجنسي من خلال العرض المرئي والسمعي مع دفع قيمة ذلك. كذلك يتم عبر الإنترنت الترويج للرقيق الأبيض وتجارة القاصرات ودعارة الأطفال بقصد الاستخدام الجنسي Cyber Teen في الوقت الذي يستمر مرتكب هذه الجريمة في حالة تخفٍّ قد لا يكون من السهولة التعرف عليه، خصوصاً إذا كان يباشر نشاطه عبر المواقع المجانية أو من خلال المجموعات الإخبارية أو القائمة البريدية[(2)].

ومن الوقائع الكبرى في مكافحة جريمة دعارة الأطفال تلك التي تعرف

(1) Conseil Federal suisse: Message concernant la modification du code penal suisse et du code penal militaire (Infractions contre l'integrite sexuelle; prescription en cas d'infractions contre l'integrite sexuelle des enfants et interdiction de la possession de pornographie dure) du 10 Mai 2000, P.7/2775.

(2) لمزيد من التفصيل في هذه القضية انظر الموقع التالي:
http://www.leeds.ae.uk/law/pgs/vaman/watchmen.htm.

لدى الشرطة الإنجليزية، بعد تدخلها في يوليو 1995 فيها بمصطلح Operation Starburst، حيث اتخذ التحقيق فيه هذه العملية بعدًا دوليًا، لاسيما وأن الإنترنت في هذه الواقعة قد استخدمت كمجال لدعارة الأطفال وتوزيع صور فاضحة للأطفال، ولقد أُدين في هذه الجريمة تسعة رجال إنجليز، كما تم الاستدلال على مجموعة أخرى عبر أوروبا وأمريكا الجنوبية وشرق آسيا وصل عدد المدانين في هذه الجريمة إلى سبعة وثلاثين شخصًا[1]. كما قامت المباحث الفيدرالية الأمريكية بالتحقيق في قضية أطلق عليها Innocent Images، وهو التحقيق الذي بدأ على إثر اختفاء طفل أمريكي، من ولاية مريلاند، في العاشرة من عمره. وهي القضية التي أُدين فيها 161 شخصًا. وفي عام 1997 كانت قضية Operation Rip Cord التي قامت بها المباحث الفيدرالية بالقبض على 1500 شخص من المشتبه فيهم بالتعامل في دعارة الأطفال عبر الإنترنت وبث صور فاضحة Child pornographers للقُصَّر. ولقد قادت عمليات البحث والتقصي حول دعارة الأطفال عبر الإنترنت، في ألمانيا والمملكة المتحدة والولايات المتحدة الأمريكية، إلى الكشف عن مائتي ألف صورة من صور دعارة الأطفال، كما تمت مصادرة مائة وسبعة وثلاثين ألف حاسوب شخصي/ منزلي Home PC. وفي عام 1998 قام البوليس الإنجليزي بعملية كبرى أطلق عليها اسم Cathedral بالتعاون مع الشرطة في 21 دولة في أوروبا وأستراليا والولايات المتحدة والبوليس الدولي/ الإنتربول لضبط حوالى مائة شخص ممن يتعاملون في دعارة الأطفال عبر الإنترنت.

وفي شهر أكتوبر 2000 قام المدعي العام الإيطالي بإحالة 1491 من الإيطاليين إلى القضاء، لكونهم قاموا بإنزال download صور دعارة أطفال Child pornography عبر الإنترنت، بعد أن قامت الشرطة الإيطالية بتفتيش ستمائة

(1) Dr.Andrzej Adamski, op. cit at 223.

منزل، وبينهم تسعة أشخاص كانوا يتاجرون في دعارة الأطفال عبر روسيا. وتعد هذه الدعوى الأكبر في إيطاليا في ذلك التاريخ، حيث قام المدعي العام الإيطالي Alfredo Ormanni بإحالة 831 متهمًا إلى القضاء الجنائي، وتم استدعاء 660 من جنسيات أجنبية ويعتقد أن أغلبهم من روسيا وفرنسا وماليزيا[1].

## ثانيًا: جريمة الترويج السمعي المرئي الفاضح في التشريع المقارن

اهتمت التشريعات المقارنة بظاهرة الترويج السمعي ـ المرئي الفاضح، وبصفة خاصة موضوع دعارة الأطفال التي أخذت من المشرع المقارن اهتمامًا كاملاً في هذا الإطار.

في الولايات المتحدة نشط الفقه والقضاء والتشريع في دراسة نظم القانون الأخلاقي وعملية نظمه في القانون الجنائي، على إثر الكارثة الحقيقية الممثلة في دعارة الأطفال عبر الإنترنت، وهي ظاهرة اعتبرت هناك خطرة على المُثُل القومية التي تقوم عليها دعائم المجتمع الأمريكي[2]! لكون الإنترنت وسيلة تجعل ارتكاب مثل هذه الجرائم سهلاً، أو بمعنى أكثر دقة؛ تجعل من الممكن ومن ثم توفِّر المناخ الملائم للحصول على ضحايا في مثل هذه النوعية من الجرائم. ومثل هذا الأمر جعل الفقه والقضاء والتشريع في الولايات المتحدة يتجه إلى الاستمرار في دراسة دعارة الأطفال عبر الإنترنت ـ وذلك بإيعاز من البيت الأبيض الأمريكي في بيانه المؤرخ 26/ 1/ 1996 الذي صدر ردًا على إلغاء

---

(1) Martin Stone, Italians charge 1491 in online pedophile sting, newsbytes, 30 Oct. 2000.
http://www.newsbytes.com/news/00/157391.html.

(2) Herb Lin, PhD hlin@nas.edu mailto:hlin@nas.edu, Michele Kipke, PhD mkipke@nas.edu mailto:mkipke@nas.edu - Tools and Strategies for protecting kids from pornography and their applicability to other inappropriate internet content, op. cit, P.1.

القضاء الأمريكي نصوصاً في قانون أخلاق الاتصالات لسنة 1996 المعدِّل للقانون الصادر في 1936[1].

ونتيجة لمبادرة البيت الأبيض المذكورة فإنه في عام 1998 أصدر الكونجرس الأمريكي القانون رقم Public Law 105-314 بشأن حماية الأطفال من التعدي الجنسي[2]. ولقد تضمن هذا القانون حثَّ النائب العام الأمريكي على التعاون مع الأكاديمية الوطنية للعلوم/ مجلس البحوث الوطنية فيها، على إعداد دراسة متكاملة لبحث مدى إمكانية تفعيل القانون الجنائي في القضايا الأخلاقية، والتي أنتجها التعامل السلبي مع تقنية المعلومات/ الإنترنت. على أن يتم وضع هذا التقرير في خلال سنتين من تاريخ صدور القانون المذكور. ولقد تم وضع التقرير في عام 2000 متضمنًا الخطوات الفعالة من الوجهة العلمية من قبل الأستاذين Herb Lin, PhD, Michele Kipke, PhD، بالتعاون مع جهات أخرى ذات علاقة. ولقد وجد التقرير أن مشكلة الدعارة المصورة Pornography ذات أساس من ناحيتين، الأولى كونها تعد داخلة في نطاق اهتمام قسم اجتماعي له دور في المجتمع، حتى وإن كان سلبيًا. أما الناحية الثانية فيتعلق بالتحديد القضائي لمصطلح الدعارة الذي يتخذ مفهوماً يتسع ليشمل الطابع المتغير فيها vary widely من نطاق اجتماعي إلى آخر Vary by community[3].

ولقد أشار الباحثان في التقرير المذكور إلى أن المشكلة يتم النظر إليها من الزاوية العائلية والمدرسية، وفيها ينبغي أن يكون هناك دور للعائلة والمدرسة في

(1) Reno v. ACLU, US Supp. 521 U.S. 844 (1997).

(2) Protection of children from Sexual predators act of 1998 Title 9 section 901. US Code. Id at 422.

(3) Herb Lin, PhD hlin@nas.edu mailto:hlin@nas.edu, Michele Kipke, PhD mkipke@nas.edu mailto:mkipke@nas.edu - Tools and Strategies for Protecting Kids from Pornography and Their Applicability to other Inappropriate Internet Content, P.4.

توعية النشء. ومن الزاوية الاجتماعية على مستوى الدولة وبحيث ينظر إليها كمشكلة تتعلق بـ. . . سلوك مستهجن Inappropriate content يضم في إطاره جميع أنواع السلوك المستهجن الأخرى والتي يمكن ارتكابها سواء عبر الإنترنت أو غيرها[1]، ومن ثم يجب التعامل مع هذا السلوك المستهجن كظاهرة كلية ليس فيها تمييز فيما لو تمت عبر الإنترنت أو في العالم المادي. حتى في ظل المنطق السائد من حيث لزوم الأخذ في الاعتبار منطق الظروف الاجتماعية في كل بيئة، وفي هذا ما يناقض اتجاهات القضاء الأمريكي في عدم إمكانية حصر أنواع السلوك المستهجن لاختلاف الثقافات، حيث كان ذلك هو السبب في نقض القانون المذكور وبما يُعدّ ذلك عودة إلى نهج قانون أخلاق الاتصالات لسنة 1996 المنقوض.

كذلك يجب الأخذ في الاعتبار ما هو مقرر في القانون الأمريكي من العقاب على توريد Import مواد فاحشة Obscene Material إلى داخل الولايات المتحدة حسبما هو مقرر في القسم 18 US Code Sec. 1462. وهذا النص الأخير يقتضي بالطبع أن تكون المواد الفاحشة قد تم إعدادها في خارج الولايات المتحدة الأمريكية، بحيث تصل إلى داخل الحدود الإقليمية بعد ذلك. ومثل هذا النص يثير مشكلتين، إحداهما تبرز حين التعرض لتحديد المواد الفاحشة التي يمكن أن تكون عرضة لمساءلة القانون، وفق هذا النص، سيما وإن هناك درعًا قويًا ممثلاً في مبدأ حرية التعبير (التعديل الأول للدستور الأمريكي) حتى وإن كان موقف المحكمة العليا الأمريكية هو أن التعديل الأول لا يحمي الفحش. وأما المشكلة الثانية فهي تتعلق بتحديد الدخول إلى الحدود الإقليمية حيث يسري القانون الأمريكي. ذلك أن هذه المواد إذا تم نقلها ماديًا فإن ذلك لن يشكل مشكلة في انطباق القانون. وكذلك إذا تم توريدها باستخدام الحاسوب وتم إخراجها منه وتداولها في داخل الولايات المتحدة، إلا أن ما

(1) Ibid.

يمكن عَدُّه مشكلة يتعلق تحديدًا بموضوع البث الآلي للمواقع الفاحشة، حيث أن بث موقع يتضمن مواد فاحشة من خارج الولايات المتحدة فإنه يصل آليًا إلى داخل الولايات المتحدة، فهل يعد مثل هذا البث الآلي توريدًا إلى داخل الولايات المتحدة؟

كذلك يحظر القانون الأمريكي تصدير Transport المواد الفاحشة ما بين الولايات أو إلى خارج الحدود الفيدرالية (18 US Code Sec. 1463).

كذلك يجرم القانون الأمريكي تشغيل Employ القُصَّر Minors أو دفعهم Induce إلى المشاركة في صور متحركة Visual depiction تتضمن حركة جنسية مباشرة، إذا كان التصوير قد تم باستخدام حاسوب عبر مؤسسات تجارية في الولايات أو في خارج الولايات المتحدة (18 US Code Sec. 2251). كذلك يحظر القانون الأمريكي استخدام الحاسوب لبيع Sell أو نقل Transfer حق الوصايا على قاصر مع العلم بأن هذا القاصر سوف يتم استخدامه لإعداد صور متحركة تتضمن سلوكًا جنسيًا مباشرًا (18 US Code Sec. 2251 A). كما يجرم القانون الأمريكي استخدام الحاسوب لنقل Transport دعارة الأطفال Child pornography عبر الولايات أو عبر مؤسسات تجارية أجنبية (18 US Code Sec. 2252 & 2252 A)[1].

أما في فرنسا فإن المادة (24 ـ 227) من قانون العقوبات الفرنسي الجديد تعد حجر الأساس في إطار دعارة الأطفال[2]. حيث يعاقب مُعِدُّ مواقع دعارة

(1) USA v. Hay, App. 9th Cir. No. 99-30101, 24 Oct. 2000, Available online in Oct. 2000 at: http://laws.findlaw.com/9th/9930101.html.

(2) Guillam Desgens - Pasanau, Au Centre des debat actuels: La protection des mineurs sur l'internet -24/7/2001. disponible enligne en Juillet 2001 a: http://www.droit-technologie.org/1.2.asp?actuid = 1604298204.

انظر القانون رقم 468 ـ 98 المؤرخ 17/ 6/ 1998 بأن منع والمعاقبة على الجرائم وحماية القُصَّر تعاقب كل من يقوم ببث مواقع دعارة أطفال.

الأطفال وفقًا للمادة (24 ـ 227) في فقرتها الأولى من القانون ذاته، أما الفقرة الثانية منها فتعاقب مستخدم الموقع.

وأما قانون العقوبات البلجيكي فقد تضمن في المادة (383 bis) منه (المضافة بالقانون المؤرخ 13/ 4/ 1995)[1] العقاب على عرض Expose وبيع Vendu وتأجير Loue وتوزيع Distribute أو دعم موقع مرئي Remi des supports Visuals لأوضاع جنسية ذات طابع فاحش Pornographique، وذلك باستخدام قُصّرٍ ممن لم يبلغوا السادسة عشرة من أعمارهم، ويعاقب كذلك مُعِدُّ مثل هذه المواقع وكذلك مستوردها[2].

وفي القانون الليبي توجد المادة (409 ـ عقوبات) التي تعاقب على تحريض الصغار دون الثامنة عشرة على الفسق والفجور أو مساعدتهم على ذلك أو التمهيد لهم أو القيام بتسهيل ارتكاب مثل هذه الأفعال أو إثارتهم بأية طريقة كانت لارتكاب فعل شهواني أو قام بارتكابه أمامهم. وعلى الرغم من الغموض الكبير الذي يكتنف عبارة (بأية طريقة كانت) الواردة في النص، فإنه مع ذلك يمكن القول بتطبيق هذا النص جزئيًا على أفعال الإثارة فقط، إذا كان الطفل على دراية بالجاني، فمثلاً لا ينطبق هذا النص على أصحاب المواقع التي تقوم بترويج دعارة أطفال، حال قيامهم ببث عام دون تحديد للمجني عليه، وإنما يلزم أن يكون هناك جان محدد يقوم باستثارة طفل أو أطفال بعينهم. ذلك أن القانون أطلق العنان للسلوك المادي المستخدم في جريمة إثارة الأطفال وحدها، والذي من الممكن أن يكون باستخدام

(1) Sur le plan penal, deux infractions contenues dans le Nouveau Code Penal (NCP), ayant pour finalite la protection des mineurs, meritent, concernant le reseau Internet, une attention particuliere. Ainsi: - «le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image d'un mineur lorsque cette image presente un caractre pornographique».

(2) Thibault Verbiest - Pornographique e Internet: comment reprimer? 19 Mai 2001, disponible enligne en juin 2001 a: http://www.droit-technologie.org/1.2.asp?actu.id = 2099182987.

الإنترنت عن طريق الاتصال بهم أو معهم والقيام بإرسال ملفات جنسية لهم وصور داعرة وحثهم عبر الاتصال المباشر والوسائل السمعية المرئية، التي برع في استخدامها النشء، بالقيام بأفعال جنسية. فمن الممكن هنا أن يقوم المجرم بإرسال ملف يتضمن ارتكابه لفعل شهواني لإثارة طفل أو مجموع أطفال، وبقصد حثهم على ارتكاب فسق وفجور، فيقوم الطفل بالإطلاع عليه، ففي هذه الحالة يكون الشخص قد ارتكب جريمة إثارة الأطفال أمامهم كما هي موصوفة في النموذج القانوني للجريمة. وقولنا هذا عائد إلى أن المشرع لم يَسْعَ إلى استنطاق الجاني لمظاهر إثارة الطفل بقصد ارتكاب فعل فاسق أو فاجر معه، وإنما معه أو مع غيره، فالجريمة المقصودة هنا في جريمة إثارة الأطفال وليس ارتكاب فعل شهواني معهم، فهذه الأخيرة يحكمها المادتان (407 ـ 408 ـ عقوبات ليبي) في حين مقصود المادة (409 ـ عقوبات ليبي) هي استثارة الأطفال شهوانيًا فقط، والمجرم يصل إلى تحقيق هذه النتيجة بأية طريقة كانت ومن ذلك القيام بتمكين الطفل من برمجيات تتعامل مع ملفات تتضمن أفعالاً فاسقة أو فاجرة وبحيث يمكن للطفل الإطلاع عليها في أي وقت[1].

---

(1) تنص المادة (409 ـ عقوبات ليبي) على إنه «يعاقب بالحبس كل من حرض صغيرًا دون الثامنة عشرة ذكرًا كان أو أنثى على الفسق والفجور أو ساعده على ذلك أو مهد أو سهل له ذلك أو أثاره بأية طريقة كانت لارتكاب فعل شهواني أو ارتكبه أمامه سواء على شخص من الجنس نفسه أو من الجنس الآخر. وتضاعف العقوبة إذا كان الجاني ممن ورد ذكرهم في المادة (407). كما تنص المادة (407 ـ عقوبات ليبي) على أنه «1 ـ كل من واقع آخر بالقوة أو التهديد أو الخداع يُعاقب بالسجن مدة لا تزيد على عشر سنوات. 2 ـ وتطبق العقوبة ذاتها على مَنْ واقَعَ ولو بالرضا صغيرًا دون الرابعة عشرة أو شخصًا لا يقدر على المقاومة لمرض في العقل أو الجسم، فإذا كان المجني عليه قاصرًا أتم الرابعة عشرة ولم يتم الثامنة عشرة فالعقوبة بالسجن مدة لا تزيد على خمس سنوات. 3 ـ وإذا كان الفاعل من أصول المجني عليه أو من المتولين تربيته أو ملاحظته أو ممن لهم سلطة عليه أو كان خادمًا عنده أو عند من تقدم ذكره، يُعاقب بالسجن ما بين خمس سنوات وخمس عشرة سنة. 4 ـ وكل من واقع إنساناً برضاه يعاقب هو وشريكه بالسجن مدة لا تزيد على خمس سنوات». كما تنص المادة (408 ـ عقوبات ليبي) على أنه» 1 ـ كل من هتك عرض إنسان باتباع إحدى الطرق المذكورة في المادة السابقة يُعاقب بالسجن مدة لا =

على أن هذا النص يحتاج إلى تطوير جزئي في منطق التعامل مع الحركة Action، فممارسة فعل شهواني أمام طفل قد يلصق في ذاكرة الطفل، ويمكن أن يكون مؤشرًا على استثارته ودافعاً إلى ارتكاب أفعال شهوانية، ليس بالضرورة مع الجاني ذاته، حيث من الممكن أن الجاني لم يكن يسعى إلى القيام بأفعال شهوانية مع الطفل ذاته، أو يكون قد قبض عليه أو يكون قد أصيب إصابة بالغة في حادث مثلاً. ففي هذه الحالة تظل جريمة المادة (409 ـ عقوبات ليبي) قائمة ويلزم تطبيقها على الجاني وإن كان يُخَتَلف في شأن طبيعة مدى اعتبار جريمة إرسال ملف أو رسالة إلى طفل صغير، بما يتوافق مع فكرةٍ بأية طريقة كانت لاستثارته شهوانيًا، ووجه الاختلاف ينحصر في تحديد طبيعة هذه الجريمة وفيما إذا كانت وقتية أم كانت من الجرائم المستمرة وهو أثر له المنطق الذي تستمد منه حركة الزمن في العالم الافتراضي Cyber Time معاييرها وبحيث يحجب عنها مفهوم الحفظ والتسجيل المعتادين، فالاحتفاظ بملف في العالم الافتراضي، كما لو ظل الملف في البريد الإلكتروني للمجني عليه، لا يعني أنه محفوظ بذات الطريقة التي يتم بها الحفظ في القرص الصلب للحاسوب. وعندنا إن الاستمرار قائم بحيث يُعد كل مرة يطّلع فيها الطفل على الرسالة أو الملف المذكور تجعل حالة الاستمرار قائمة، لأن المشرّع لم يتطلب أكثر من مجرد التحريض أو المساعدة سوى التمهيد أو الاستثارة أو أن يكون قد ارتكب أمامه بقصد دفعه إلى ذلك غريزيًا دون أن يكون هناك تطلّب لتحقق نتيجة محددة وهي قيام الطفل المذكور بارتكاب هذه الأفعال، فيكفي في هذا الشأن ارتكاب النشاط المادي المكوّن لهذه الأفعال المجرمة.

= تزيد على خمس سنوات. 2 ـ وتطبق العقوبة ذاتها إذا ارتكب الفعل ولو بالرضا مع من كانت سنه دون الرابعة عشرة أو شخصًا لا يقدر على المقاومة لمرض في العقل أو الجسم، فإذا كانت المجني عليه بين الرابعة عشرة والثامنة عشرة كانت العقوبة الحبس مدة لا تقل عن سنة. 3 ـ وإذا كان الفاعل أحد الأشخاص المذكورين في الفقرة الأخيرة من المادة السابقة تكون العقوبة مدة لا تجاوز سبع سنين. 4 ـ وكل من هتك عرض إنسان برضاه يُعاقب هو وشريكه بالحبس».

إن مسألة تحديد القيم الاجتماعية الاقتصادية من الموضوعات التي ينظر إليها في القانون المقارن على أساس كونها تمثل صلب الحدث الرئيسي في إطار تفاعل القانون مع المجتمع في كل دولة. ويهتم المشرع والقضاء في القانون المقارن بالقيم الاجتماعية الاقتصادية لأنها تعد نقطة الارتكاز في الدفاع عن حركة المصالح الاجتماعية الاقتصادية، حيث يكون تفسير المصلحة على ضوء المفهوم الاجتماعي الاقتصادي للوقائع الإنسانية.

ففي القضاء الأمريكي فإن المبدأ العام الذي يسير عليه هو النظر إلى تحديد المقياس الاجتماعي لتحديد الفعل الفاضح أو الفاحش Obscenity حيث كان القضاء الأمريكي قد وضع معيار الفحش في قضية Miller v. California, 413 U.S. 15 (1973) بحيث يتم اختبار الفحش وفق البحث في معيار الرجل العادي Average Person وذلك ـ من ناحية ـ بتطبيق الضوابط الاجتماعية المعاصرة Contemporary community standards، والتي يمكن بمقتضاها النظر إلى أن العمل ككل يؤدي إلى المتعة الشهوانية Prurient Interest، ومن ناحية أخرى النظر فيما إذا كان النشاط يصور Deplet أو يصف Describe بطريقة عنيفة Patently offensive السلوك الجنسي Sexual conduct كما هو محدد في قانون الولاية. ومن ناحية ثالثة ينظر فيما إذا كان النشاط ككل ينقصه القيم الأدبية والاجتماعية والسياسية والعلمية[1]. والحقيقة إن منطق القيم الاجتماعية يعد عامل ارتكاز حقيقي في تفسير القانون وفق احتياجات المجتمع ككل، ومثل هذا الأمر يقود إلى البحث في القيم الأساسية للمجتمع لبحث درجة الإجرام وتفسير العمل غير المشروع، وبما يؤدي ذلك إلى سلوك مذهب تفسير القانون بحسب

---

(1) «The average person applying contemporary community standards' would find that the work, taken as a whole appeals to the prurient interest»; (2) it «depicts or describes, in a patently offensive way, sexual conduct specifically defined by applicable state law»; and (3) «the work, taken as a whole, lacks serious literary, artistic, political, or scientific value». Miller v. California, 413 U.S. Supreme Court.

المتعارف عليه في المجتمع. ومثل هذا الأمر يقود بالضرورة إلى مسألة المجتمع ذاته في القانون، وهي مسألة كنا قد تعرضنا لها حين التطرق إلى موضوع المجتمع الذي يلتزم بالدفاع عن حقوقه فيما سلف.

أما القانون الفرنسي فإنه يقرر في تشريعه أهمية جعل الأطفال القُصّر في موقع مراقبة مستمرة من قبل الأهالي، لاسيما السلطة الأبوية والمنزلية، حيث يشير الفقه القانوني إلى ضرورة قيام القائم بالسلطة الأبوية Titulaires de l'autorite parentale بدور رئيسي في مراقبة القاصر أثناء اتصاله بالإنترنت[1]. وإذا تأملنا القانون الإنجليزي فإننا نجد في القضاء هناك أنه كان له دور كبير في طرح مشكلة تطوير نصوص القانون الذي يتعلق بترويج مواد الدعارة باستخدام الحاسوب والإنترنت[2]، ولقد احتاج الأمر إلى تطوير تشريعين بداية هما قانون الفحش العلني لسنة 1959 The protection of Children act. ولقد تم تعديل هذه التشريعات بمقتضى قانون العدالة الجنائية والنظام العام لسنة 1994 The Criminal Justice & Public Order Act 1994 لكي يتلاءم مع لغة عصر المعلوماتية[3].

## المبحث الخامس:
## جرائم البث العلني

يُعد البث العلني Diffusion en Publique، أحد الخصائص التي تتميز بها تقنية الإنترنت، باعتبارها أكبر حدث علمي بارز منذ اختراع الطباعة. فهي فضلاً عن كونها وسيلة حية، وأيضًا حيوية، للبث فيها فإنها اجتمعت فيها مظاهر البث

(1) Guillam Desgnes - Pasanau, op. cit., P.4.
(2) R. v. Fellows & Arnold App. England, 1997, See: Paul Cullen QC - Computer Crime, op. cit., at 213.
(3) Id.

السمعي المرئي Audiovisual أيضًا، فاحتوت بذلك قوة وسائل وأدوات البث التقليدية (المقروءة ـ المسموعة ـ المرئية). فإذا أضفنا إلى ذلك الظاهرة العلنية التي عليها الإنترنت، من حيث كونها إحدى وسائل العلنية كما عرّفها قانون العقوبات، إن لم تكن أقواها على الإطلاق، فإن ذلك ليعبر عن القدرة الإيجابية ذات الطابع الفريد للإنترنت. لذلك يمكن عداد الإنترنت وبما تحويه من عالم افتراضي وسيلة يمكنها أن تستوعب حركة البث في مظاهرها كافة .

وعلى الرغم مما سلف فإن نقطة واحدة تظل في منأى عن اتصالها بالإنترنت وهي الالتقاء المادي المباشر بين الأشخاص، وهذه يُبنى عليها تفرقة مادية في الحدث يمكن أن يكون لها تأثيرمادي ولكن لا يمتد إلى القانون. والفرض هنا بالطبع إمكانية حدوث اتصال مرئي بين شخصين فأكثر وينطبق على المكان، إما الوصف الخاص وإما الوصف العام للمحل، فمثلاً يمكن أن يجتمع عبر الإنترنت عدة أشخاص لكي يتبادلوا أطراف الحديث بالرؤيا المباشرة في ذات الوقت، بحيث يرى أحدهم الآخر أو أنهم جُلُّهم يرى بعضُهم بعضاً ومثال ذلك النظام المؤتمري أو حلقة النقاش News group أو Conference، وفي هذه الحالة تتوافر صفة العمومية إذا كان المؤتمر المذكور مما يسمح بالولوج إليه من قبل أي كان، فهو في هذه الحالة من الأماكن العامة طالما وجد ما يدل على إمكانية الاشتراك في هذا المؤتمر أو حلقة النقاش حتى بمجرد المتابعة لما يجري، وهو أمر ينطبق عليه مدلول العلنية (16/ 1 ـ عقوبات ليبي).

ويتخذ البث الفاضح العلني مظاهر عدة، إلا أنها تتوحد كلها عبر الإنترنت في كونها بثًا، وهو أمر يُستفاد منه أنّ التمييز الحادث بين مظاهر البث هو تمييز حادث في العالم المادي ومصدره القانون، وهو أمر يجد له أثرًا عبر الإنترنت أيضًا، إذ يميز هناك بين كون البث نشرًا، وبين كونه سبًا أو قذفًا أو تشهيرًا، وبين كونه مراسلة بريدية عبر البريد الإلكتروني، وفيما إذا كان هناك علنية أم لا،

وفيما إذا كانت العلنية مفترضة في أي من هذه الحالات من عدمه، وذلك لما توفره الإنترنت من مجموعة بدائل تستخدم في التعامل عبرها. على أنه يلاحظ أن المشرع في بعض الأحيان لا يستجيب للعلنية، وتالياً نجدها غير متطلبة على الرغم من طبيعة الجريمة هنا وكونها من طبيعة الجرائم الفاضحة، والتي تسبب تصغيرًا من شأن المجني عليه عند أهل مهنته وبني وطنه. ومع ذلك تتكامل هذه الجريمة ويكون الجاني عُرضةً للإدانة دونما اعتبار لما إذا كان هناك علانية من عدمه، مثل ما هو مقرر في جرائم إهانة الصحفي أو التعدي عليه بسبب عمله، والتي لم يتطلب فيها القانون العلانية. ومن ثم فإنه سواء توافرت العلنية أو لم تتوافر فإن الجريمة قائمة، وهو ما تنص عليه المادة (12) من القانون رقم 96 لسنة 1996 بشأن الصحافة في مصر؛ من أنه «كل من أهان صحفيًا أو تعدّى عليه ـ بسبب عمله ـ يعاقب بالعقوبات المقررة لإهانة الموظف العمومي أو التعدي عليه في (المواد 133 ـ 136 ـ 137/ 1) من قانون العقوبات ـ بحسب الأحوال».

وهنا سوف نتطرق إلى موضوع البث العلني في أشكاله التي تمّ رصدها فيما سلف، وهي النشر Publication والسبّ والقذف والتشهير Defamation والمراسلة Mailing وذلك في الفقرات التالية:

**أولاً: النشر**: ليس المقصود بالنشر هنا هو النشر الصحفي عبر الإنترنت، وإنما مقصوده قيام أي شخص بنشر ما يمكنه أن يقوم به مباشرة تجاه أي شخص، فالنشر المقصود هنا لا يقع في نطاق العمل الصحفي فقط، وإنما بث مباشر على الإنترنت بخطاب مباشر مع الآخرين.

فالنشر عبر الإنترنت ليس هو النشر في العالم المادي، ففي العالم الافتراضي يكون النشر متميزًا بخاصية الحرية المطلقة غير المقيدة بإجراءات، سوى تلك التي تتعلق بحجز نطاق اسم Domain Name ثم حجز المساحة اللازمة على الإنترنت لدى أحد مزودي الخدمات، وهذه وتلك متوافرة ويمكن

القيام بها بسهولة تامة دونما حاجة لكي يكون التأجير من قبل مزود خدمات وطني، بل يمكن القيام بحجز نطاق الاسم والمساحة المرغوبة من مزود دخول في دولة أخرى إن لزم الأمر، والقيام بالبث مباشرة كما لو كان ذلك من مزود دخول بجوار المنزل. فلا يهم فيما إذا كان مزود الدخول في آخر العالم أو كان في الشارع الخلفي لمحل إقامة المتهم. ثم يتم بعد ذلك القيام بالبث بأي شكل من الأشكال. فإذا تضمن البث سبًا أو قذفًا فإن الأمر يتطلب هنا دراسة النصوص للنظر فيما إذا كانت تتناسب مع مثل هذا الحدث أم أنها ليست متناسبة، وهو الأمر الذي يستدعي تدخل المشرّع في هذا الشأن. والحقيقة أن النشر عبر الإنترنت إنما هو أقرب إلى البث منه إلى النشر المتعارف عليه في العالم المادي. إذ أن إجراءات النشر عبر الإنترنت لا يتطلب فيها اتخاذ الإجراءات التي يتطلبها القانون للنشر بالمعنى الضيق في العالم المادي، فمثلاً لا يستدعي النشر عبر الإنترنت لزوم اتخاذ إجراءات إيداع المصنف كما هو مقرر في العالم المادي، كما أنه لا يلزم أن يكون النشر محاطًا بضمانات النظام العام والآداب. . .الخ. فمثلاً يستطيع أي شخص إنشاء صحيفة عبر الإنترنت، دون لزوم اتخاذ الإجراءات القانونية التي يتطلبها القانون لنشر صحيفة في العالم المادي، وفي هذه الحالة سوف يكون في حل من المساءلة مادامت الصحيفة رقمية. بل أن النشر عبر الإنترنت إنما هو أقرب إلى ممارسة الحرية الكاملة في البث منه إلى النشر، بحيث يخضع الأمر لذوق عضو الإنترنت المطلع على ما يتم نشره. ولذلك آثار في القانون من حيث اقتراب مفهوم النشر عبر الإنترنت من المنطق الواسع له الذي يتخذ شكل البث الكامل بكل حرية. وهذا المفهوم الواسع للنشر عبر الإنترنت يجعل انطباق المدلول الموسع للنشر في قانون العقوبات متوافقًا معه، فمثلاً في القانون الليبي فإن النشر غير المشروع يمكن أن يشكل جريمة وفقًا للمواد (274 ـ 290 ـ 291 ـ 317 ـ 318 ـ 319 ـ 320 ـ عقوبات ليبي). كما يتولى القانون المؤرخ 29/ 7/ 1881 بشأن الصحافة في فرنسا العقاب على البث الإجرامي العلني إذا تم عبر الإنترنت بأسلوب السمعي

البصري Audiovisuelle كما لو تم هذا البث عبر إحدى حلقات النقاش مثلاً Forum de Discussion [1]. ومع ذلك يُعتد بّالتقادم الصحفي الاستثنائي في حالة النشر لما يتضمن قذفًا عبر الإنترنت، وهو التقادم المقرر في المادة (65) من قانون 29 يوليو 1881[2].

إن البث عبر الإنترنت لا يتطلب سوى إعداد العدة الخاصة بذلك للقيام به، من حيث اختيار نطاق اسم بحجزه لدى الجهة المختصة، ثم القيام بإعداد موقع[3] لذلك باستخدام تكنولوجيا المعلومات/ الحاسوب والبرمجيات والبيانات تحديدًا، ثم استخدام قرص صلب أو مرن أو مضغوط، ممغنط، لكي يتم نقله وإيداعه في الحاسوب الخادم أو الملقم، ثم بعد ذلك استخدام برمجيات أخرى لكي يتم تحميل ذلك على الإنترنت، وذلك يتم بطريق الحيازة المشروعة لمساحة في مضيف، مع ضرورة حيازة برمجيات أخرى[4] يمكن بطريقها القيام بإنزال هذا الموقع عند الحاجة لإجراء تعديل ما في هذا الموقع.

(1) وفي إطار القانون الفرنسي فإنه يلزم الأخذ في الاعتبار بأن القانون المؤرخ 29/ 7/ 1881 بشأن حرية الصحافة بعد القانون الأساسي الذي يتشكل معه النظام القانوني للصحافة Le Cadre Legal de la press. وهو القانون الذي تم سنّه من قبل مشرع الجمهورية الثالثة، بحيث يمكن القول أنه متوافق مع الإعلان الفرنسي لحقوق الإنسان والمواطن في المادة (11) منه التي تنص على حرية الإنسان في بث أفكاره وآرائه كما له حرية الكلام والكتابة والطباعة شريطة ألا يكون في هذه الحرية تعسّف من أي نوع. ولقد تم تعديل القانون المذكور بمقتضى القانون المؤرخ 29/ 7/ 1982 بشأن الاتصالات السمعية المرئية ثم بمقتضى القانون المؤرخ 1/ 8/ 1986 بشأن هيئة النظام القانوني للصحافة ثم أضيف إلى هذه النصوص القانون المؤرخ 13/ 7/ 1990 بشأن العنصرية، وهو القانون المعروف باسم تشريع Loi Gayssot.

(2) Cass. Cr. 30/1/2001, No.655, Disponible enligne en Oct. 2001 a: http://www.juriscom.net

(3) Stephane Liti - Le Changement d'adresse sans demenagement, Nouvelle cause dirresponsabilite penale, commentaire du jugement rendo par la 17eme ch. Corr. Du TGI de Paris, le 28 Jan. 1999, disponible en ligne a: http://www.legalis.nt/inet/commentaires/lilti-280199.htm.

(4) Uploader - Downloader.

ويترتب على هذا الاختلاف المادي في البث عبر الإنترنت وبين النشر في العالم المادي أثر قانوني هام يتعلق بتطبيق التقادم على نوعية الجرائم التي ترتكب عبر بث الإنترنت، مثلما هو الحال فيما يتعلق بتطبيق المادة (65) من قانون الصحافة الفرنسي. إذ إن التقادم بثلاثة أشهر المقرر في هذا القانون يسري من تاريخ النشر المادي لموضوع الجريمة في حين أن التقادم لا يسري على جرائم البث عبر الإنترنت، وإن كان هناك رأي يذهب إلى القول بأن التقادم يسري كما هو الحال في جرائم النشر المادي، إلا أنه يتجدد كلما كان هناك تغيير للخادم المضيف الذي وضع فيه الموقع الذي يحتوي على جرائم البث من قبل، وذهب هذا الرأي إلى التأكيد على أن مجرد تغيير نطاق الاسم Domain Name يؤدي بالضرورة إلى تحديد التقادم المشار إليه[1].

**ثانيًا: السب والتشهير**: تُعد هذه الجرائم من أقدم الجرائم المرتكبة عبر الإنترنت، وذلك لما يتمتع به عضو الإنترنت دائماً ـ وبحسب المعتقد السائد ـ من حرية كاملة عبر الإنترنت، لذا يجب ألا نستغرب إذا كنا قد ارتكبنا أيًا من الأفعال المشار إليها عبر الإنترنت في المساء، لنجد في صباح اليوم التالي دعوى تباشر ضدنا في إحدى المحاكم وإعلانًا بالحضور لسماع الحكم علينا لأنه في يوم. . . . الخ.

**(أ) السبّ**: وهو خدش شرف شخص أو اعتباره في حضوره، وذلك بتوجيه كلمات مقذعة في مواجهة شخص أو أشخاص معينين بدقة كافية[2]، على أن يكون حاضرًا كل من الجاني والمجني عليه الواقعة، ويشمل السب والقذف نسبة وقائع معينة لكي يصل إلى مجرد توجيه عبارات تعد خدشًا للشرف والاعتبار دون أن يكون فيه إسناد لواقعة معينة كما هو الشأن فيما هو مقرر في

(1) Stephane Lilti, op. cit.

(2) طعن جنائي مصري رقم 20471 لسنة 60 ق جلسة 14/ 11/ 1999. المحامي/ مصر ع. 1 لسنة 2001، ص206.

المادة (306 ـ عقوبات مصري)[1]. وإن كان بعضُ التشريعات يتطلب أن تكون الواقعة علنية، وذلك مثلما هو الحال فيما تقضي به المادة (R-624-4) من قانون العقوبات الفرنسي الجديد التي تنص على أنّ «السبّ غير العلني الواقع في مواجهة شخص أو مجموعة أشخاص بسبب الأصل أو الانتماء أو عدم الانتماء، حقيقةً أو مفترضاً، على عِرضٍ أو أمةٍ أو عنصرٍ أو دينٍ محدّدٍ، معاقب عليه بالغرامة المقررة على الجنحة من المستوى الرابع»[2].

أما القانون المؤرخ 29/ 7/ 1881 بشأن حرية الصحافة فإنه يُعرّف السبَّ بأنه «كل تعبير مهين أو شائن، أو مصطلحات احتقار أو قدح التي لا تؤدي إلى الاتهام بأي فعل»[3].

وكانت المادة (308 مكرر ـ عقوبات مصري) التي تنص على أنه «كل من قذف غيره بطريق التليفون يعاقب بالعقوبات المنصوص عليها في المادة 303. وكل من وجه إلى غيره بالطريق المشار إليه بالفقرة السابقة سبًا لا يشتمل على إسناد واقعة معينة بل يتضمن بأي وجه من الوجوه خدشًا للشرف أو الاعتبار يعاقب بالعقوبة المنصوص عليها في المادة 306. وإذا تضمن العيب أو القذف أو السبّ الذي ارتكب بالطريق المبين بالفقرتين السابقتين طعنًا في عِرض الأفراد وخدشًا لسمعة العائلات يعاقب بالعقوبة المنصوص عليها في المادة 308»[4].

---

(1) طعن جنائي مصري رقم 12952 لسنة 60ق جلسة 22/ 2/ 2000. المحامي/ مصر ع. 1 لسنة 2001، ص206.

(2) Art (R-624-4-CPN Fr.) «L’injure non puplique commise envers une personne ou un groupe de personnes a raison de leur origine ou de leur appartenance, vraie ou supposee, a une ethnic, une nation, une race ou une religion determince est punie de l’amende prevue pour les contraventions de la de classe».

(3) L’article 29 de la loi du 29 Juillet 1881 definit l’injuire comme «toute expression outrageante termes de mepris ou invective qui ne renferme l’imputation d’aucun fait».

(4) انظر في ذلك: د. جميل عبد الباقي الصغير، الأحكام الموضوعية، المرجع السابق، ص29.

على أن المشرّع قد يتوسع في مسألة الحضور المادي للمجني عليه، بحيث يكون السبّ متوافرًا إذا لم يكن المجني عليه حاضرًا ماديًا بشخصه، مثلما هو الحال فيما تقضي به المادة (306 ـ عقوبات مصري) من أن «كل سب لا يشتمل على إسناد واقعة معينة بل يتضمن بأي وجه من الوجوه خدشًا للشرف أو الاعتبار يعاقب عليه في الأحوال المبينة بالمادة 171 بالحبس مدة لا تتجاوز سنة وبغرامة لا تقل عن ألف جنيه ولا تزيد على خمسة آلاف جنيه أو بإحدى هاتين العقوبتين».

المادة (438 ـ عقوبات ليبي) التي تنص على أنه «كل من خدش شرف شخص أو اعتباره في حضوره يعاقب بالحبس مدة لا تجاوز ستة أشهر أو بغرامة لا تجاوز خمسة وعشرين دينارًا. وتطبق العقوبات ذاتها على من ارتكب الفعل بالبرق أو التليفون أو المحررات أو الرسوم الموجهة للشخص المعتدى عليه. وتكون العقوبة الحبس لمدة لا تجاوز السنة أو الغرامة التي تجاوز أربعين دينارًا إذا وقع الاعتداء بإسناد واقعة معينة».

وفي قانون العقوبات الإيطالي تعاقب المواد (594 ـ 595) على السب. كما تضمن القانون الأمريكي نصًا هو 47 Sec. 223 (a) يعاقب على استخدام عبارات قذرة إذا كان الغرض منها مضايقة Annoy الغير[1].

**(ب) التشهير**: والتشهير Libel من جرائم البث المباشر في القانون، وهو في كل الأحوال نوع من القذف، وإن كان يستلزم في القانون الأمريكي أن يكون كتابةً. في حين أن التشهير بالكلام يُطلق عليه في المصطلح الأنجلوفوني Slander. فالأساس الذي يعتمد عليه التشريع الأمريكي في إطار التشهير ينطلق من تهديد سمعة شخص ما Man's Reputation التي تمثل المصلحة التي يحميها القانون هنا. حيث يؤدي التشهير إلى التقليل من قدر الشخص في نظر المجتمع

(1) USA v. William M. Landham, 2001 FED App. 01 75P (6th Cir.), No. 99-5471, May 25, 2001.

والناس أيًا كانوا، مثل أقاربه وجيرانه والأشخاص الذين لهم علاقة بهم أيًا كانت نوعية هذه العلاقة، كما لو كانت هذه العلاقة عائلية أو شخصية أو تجارية أو مالية. . .الخ.

وهو الأمر ذاته في القانون الفرنسي، فالمادة (R. 624-3) من قانون العقوبات الفرنسي الجديد تنص على أنّ «القذف غير العلني يقع في مواجهة شخص أو مجموعة أشخاص بسبب أصلهم أو انتمائهم أو عدم انتمائهم، الحقيقي أو المفترض، إلى عِرق أو أمّة أو جَذر أو دين»[1]. كما تنص المادة (439 ـ عقوبات ليبي) على أن يعاقب بالحبس مدة لا تزيد على سنة أو بغرامة لا تجاوز خمسين دينارًا كل من اعتدى على سمعة أحد بالتشهير به في غير حضوره لدى عدة أشخاص، وذلك في الأحوال المنصوص عليها في المادة السابقة. وإذا وقع التشهير بإسناد واقعة معينة تكون العقوبة الحبس الذي لا تتجاوز مدته السنتين أو الغرامة التي لا تجاوز السبعين دينارًا. وإذا حصل التشهير عن طريق الصحف أو غيرها من طرق العلانية أو في وثيقة عمومية، تكون العقوبة الحبس الذي لا يقل عن ستة أشهر أو الغرامة التي تتراوح بين عشرين دينارًا ومائة دينار. وإذا وُجِّه التشهير إلى هيئة سياسية أو إدارية أو قضائية أو إلى من يمثلها أو إلى هيئة منعقدة انعقادًا صحيحًا، لتزاد العقوبة بمقدار لا يجاوز الثلث».

**ثالثًا: السبّ عبر الإنترنت**: إذا كان الفقه والقضاء قد وجدا صعوبات حال البحث عن معيار يمكن بمقتضاه التمييز بين ما هو مقرر في التشريع من تمييز بين الطريقة التي يمكن بها ارتكاب السب والقذف[2]، فإن الأمر استقر فيما يبدو

(1) La diffamation non puplique commise envers une personne ou un groupe de personnes a raison de leur origine ou de leur appartenance ou de leur non-appartenance, vrai ou supposee, a une ethnie, une nation, une race ou une religion determinee est punie de l’amende prevue pour les contravention de le 4e classe».

(2) David Loundy - Computer information systems Law & system Operator Liabilty, the Seattle Uni. Law Review, Vol. 21, No.4, Summer 1998, P.16.

على المعيار الاحتياطي الدائم، وهو معيار واقعي مستمد من البحث في كل حالة على حدة، وذلك لصعوبة التمييز بين السب والتشهير في الحالة الواقعية التي يكون فيها الفرد قائمًا وحاضرًا أمام الجاني.

أما في الحالة الاعتبارية فإن المشرع كثيرًا ما يقوم بتحديد حالات يكون فيها المجني عليه غير حاضرٍ واقعةَ السب حضورًا ماديًا كاملاً وإنما جزئيًا بحيث يستشعر أحد/ أعضاء المجني عليه واقعة السب كما هو الشأن في سماعة ورؤية واقعة السب عبر الاتصال الهاتفي والهاتف المرئي أو البرقي أو الكتابة في مُحرّر أو إعداد رسوم ما، في حين إن التشهير يلزمه، فضلاً عن عدم وجود الشخص أو حضوره الواقعة، أن ترتكب أمام عدة أشخاص، كما يمكن أن ترتكب في الصحف أو غيرها من طرق العلانية أو في وثيقة عمومية، إذ كل ما يتطلبه المشرّع في واقعة التشهير ألا يكون المجني عليه حاضرًا. أما إذا كان الشخص حاضرًا فإن الواقعة في هذه الحالة تكون سبًا وليست تشهيرًا.

لذلك فإن النطاق المادي لبحث مدى توافر واقعة السب وتمييزها عن التشهير يستلزم الحضور المادي كليًا أو جزئيًا لواقعة الجريمة، حتى يمكن القول بأن الواقعة تكون جريمة سب أو جريمة تشهير. ففي واقعة السب والقذف فإن الركن المادي يتم بناؤه على أساس تحديد شخص المجني عليه وتعيينه التعيين الكافي لا محل معه للشك في معرفة شخصيته[1]. على أن الأمر هنا ليس بهذه السهولة عبر الإنترنت، ذلك إنه لما كان من الصعوبة، إن لم يكن من المستحيل، توافر الحضور الكلي للمتهم والمجني عليه حتى يمكن القول بوجود سبٍّ ما، فإن المسألة يمكن أن تكون محل جدل فيما يتعلق بارتكاب السب الجزئي. ذلك إنه يختلف الحال حول هذه المسألة فيما إذا كان المجني عليه حاضرًا على الإنترنت وفي حالة اتصال مباشر مع الجاني، كما لو كان الاثنان

---

(1) طعن جنائي مصري رقم 20471 لسنة 60 ق جلسة 14/ 11/ 1999 (المحامي ـ صر العدد 1 لسنة 2001، ص209).

معًا في إحدى حلقات النقاش، وما إذا كان الاتصال مباشرًا بينهما أم إن الجاني يتحدث مع آخرين دون حضورٍ للمجني عليه (تشهيرٌ) أم بحضور المجني عليه (سَبٌّ) حسب الأحوال.

ومما يدخل في إطار التشهير قيام الجاني، ولو باستخدام الاستعارة، ببث رسالة باستخدام حلقات النقاش[1] وكذلك عبر قوائم المراسلة Mailing List التي تذخر بها المواقع عبر الإنترنت للتعبير عن الرأي أو الفكرة وكذلك البريد الإلكتروني[2] إلى عدد غير محدود، وفي هذه الحالة يستفيد المجني عليه من الاحتمال إذا وصلته نسخة من هذه الرسالة. أما إذا لم تصله فإن الأمر يظل في إطار التشهير كقاعدة، وفي هذه الحالة فإن المثار هنا هو موضوع العلانية التي نرى توافرها عبر الإنترنت، إذ كل ما يتطلبه المشرع في التشهير أن تكون واقعته قد تمت لدى عدة أشخاص، دون استلزام لما إذا كان حضورهم المادي متطلبًا أم لا، وهو غير الأمر فيما يتعلق بالمحرَّرات حيث يلزم أن يعترف المشرع بالوجود الرقمي لهذه المحررات. وتُعد حلقات النقاش والقوائم البريدية أو التراسلية مجالاً حيويًا لتطبيق قانون النشر الصحفي على وقائع التشهير عبر الإنترنت في فرنسا بمقتضى القانون المؤرخ 29/ 7/ 1881 بشأن الصحافة المعدل بالقانون المؤرخ 1986. فالقانون الأخير يميز بين القذف وبين الإساءة بالسب وفقًا للمادة (29) منه، حيث تُعرّف المادة الأخيرة القذف بأنه كل ادعاء أو اتهام بفعل يجلب عدواناً على سمعة أو اعتبار لشخص ما أو لمجموعة ينسب إليها الفعل»[3]. على أن السؤال الأكثر إثارة للجدل يتعلق بموضوع مضمون الرسالة التي يمكن أن تكون مجرمة بمقتضى التشريعات المختلفة في هذا الإطار.

---

(1) Guillame Desgens - Pasanau - Du Bon Usage d'un Forum de discussion, P.3- disponble en ligne en 13 Mars 2001 a : http://www.droit-technologiw.org.

(2) David Loundy, op. cit., at 17.

(3) L'article 29 de la Loi du 29 juillet 1881 definit la diffamation comme «toute allegation ou imputation d'un fait qui porte atteinte a l'honneur ou a la considera-tion de la personne ou du corps auguel le fait est impute».

**رابعًا: تكوين المراسلة الإلكترونية مجرمة:** يُعد نظام التراسل فحوى الاتصال بالإنترنت، وإذا كانت التطورات المعاصرة في تكنولوجيا المعلومات قد وصلت إلى حدود الاتصال الفوري بالصوت والصورة، بحيث يُجعَل الإنسان في حركة اتصالية مباشرة مع الغير، دونما اعتبار لما إذا كان هناك حاجز مادي من أي نوع، فإن مثل هذا الأمر بالطبع لن يترتب عليه تراجع من أي نوع أيضًا لنظام التراسل عبر الإنترنت. ولذلك عدة أسباب أبرزها على الإطلاق مسألة الاعتراف القانوني بموضوع الرسالة الإلكترونية تحديدًا حيث أخذت الرسالة الإلكترونية حظها القانوني ووصلت إلى مستوى الرسمية في هذا الإطار، بحيث يمكن تقديمها كدليل أمام المحاكم وذلك كنتيجة طبيعية للاعتراف القانوني المذكور بمخرجات الحاسوب.

والمراسلة الإلكترونية يتسع مدلولها لما هو أبعد من الرسالة التي تبث عبر الإنترنت في صيغة رسالة عبر نظام البريد الإلكتروني. إذ يتسع مدلولها ليصل إلى قائمة التراسل أو ما يطلق عليها في المصطلح الإنجليزي Mailing List، وهو نظام تراسلي جماعي يمنح صلاحية بث رسالة إلى مجموعة من الأشخاص، قد تجمعهم أفكار مشتركة حول موضوع ما أو موضوعات متعددة، قاموا بتسجيل بريدهم الإلكتروني مسبقًا في هذه القائمة، بقصد تناول هذا أو ذاك الموضوع، فيقوم هذا النظام ببث هذه الأفكار التي أرسلها هذا أو ذاك العضو في هذه القائمة لكل من يشترك فيها من أشخاص دونما حاجة لأن يكون على دراية بهم أو بشخصياتهم. وغني عن البيان أن مثل هذا النظام التراسلي كان قد نشأ في ظل أفكار العمل الجماعي، بحيث يتم تداول الأفكار في إطار المنظمة الواحدة حول موضوع ما، فهو في الحقيقة نظام مشجع للعمل الجماعي، حال تطلب وجود أكثر من رأي فيما يخص أحد الموضوعات.

ومما يندرج في إطار التراسل الإلكتروني أيضًا، كأثر لاتساع مدلوله عما

هو عليه الحال في العالم المادي، ما يسمى بنظام حلقات النقاش Newsgroups، وهي تتناول في موضوعها جلسة لمناقشة موضوع أو موضوعات فورية، أو حديث الساعة. وقد تكون في إطار مجموعة على معرفة بأحدهم الآخر، بحيث يكون دور الدخيل مجرد دور استفهامي، وبحيث يترك سؤالاً فقط لأحد المناقشين دون أن يتدخل في موضوع المناقشة حيث يكون ذلك غير مسموح به، أو أن يسمح في مثل هذه المجموعات للغير بالدخول في حلقة النقاش فيطرح أفكاره علنًا على مجموعة النقاش هذه، كما لو كان الأمر مباحًا للجميع في المشاركة. والواقع أمام تعدد أنواع وبدائل النظام التراسلي عبر العالم الرقمي، فإن الأمر يبرز كما لو كان هناك نوع من الخلط، وبحيث يطغى هذا الخلط على تحديد التكييف المناسب للعدوان في هذا الإطار، وفيما إذا كان الأمر ينطبق عليه مفهوم الرسالة كما هي معرّفة في العالم المادي، أم أن لها مفهوما آخرًا موسعًا، وبحيث يكون مدلوله متوافقًا مع الصورة التي يمكن استخدامها بها في العالم الرقمي.

والجدير بالملاحظة هنا، أن القانون الجنائي المقارن يأخذ في الاعتبار الكيفية التي يتم بها التراسل ماديًا، دون أهمية لعامل الوقت، وبحيث يعد زمن الاتصال يبدو كما لو لم يكن له قيمة في هذا الشأن. إذ عديدةٌ هي النصوص التي تشتبه على الكتابة، مثل الإبراق والفاكس والاتصالات الهاتفية، ومن ذلك ما هو مقرر في تشريع ولاية أركانساس الأمريكية ARK CODE ANN. 5-41-108 (2000) الذي يعترف بارتكاب جريمة التخويف أو الترهيب أو التهديد أو الإساءة ضد أي شخص باستخدام البريد الإلكتروني أو أية وسيلة اتصال أخرى، أو أن يقوم الشخص بارتكاب جريمة بالمراسلة حال إرسال رسائل دعاية مثيرة وغير منظمة Unsolicited bulk email باستخدام شخصية وهمية Forged identity، مثلما هو الحال في تشريع إلينوي Illinois الذي يعاقب على تزييف أو تزوير Falsifies or forges التحويل المعلوماتي بطريق الرسالة الإلكترونية بأية

مضمون، حال كون موضوع هذا التراسل بريد تافه عبر الإنترنت غير معروف مصدره.

وعليه يتسع مدلول الرسالة المجرّمة عبر الإنترنت لكي تشمل في محتواها ليس فقط جرائم الأخلاق، وإنما أيضًا جرائم أخرى تتخذ الطابع التقليدي، كما هو الشأن في جرائم التهديد بالقتل أو بارتكاب جريمة ضد النفس والمال. كما يتسع أيضًا مدلولها في إطار الجريمة التقنية بحيث تتخذ أبعادًا تقنية محضة، كما هو الشأن في تخريب قواعد البيانات أو هدم نظام المعلومات باستخدام الرسائل الإعلانية مجهولة المصدر. ولعل أشهر قضية تهديد هي تلك التي قام بها Christopher James Reincke (18 عامًا) طالب في جامعة Illinois بالولايات المتحدة الأمريكية، حيث قام في 4/ 12/ 2001 بإرسال رسالة عبر البريد الإلكتروني إلى الرئيس كلينتون وقام بتهديده فيها بالقتل.

وفيما يتعلق بطبيعة العبارات التي استخدمت في السب والقذف، فإنه لا يختلف حالها عما هو عليه الحال في العالم المادي، إذ تستخدم العبارات ذاتها التي يتم استخدامها في العالم المادي في جرائم السب والقذف والتشهير عبر الإنترنت. ولا يُقدَح هنا في عملية التغاير والاختلاف الاجتماعي والثقافي بين الشعوب للقول بعدم إمكانية تحديد مفهوم العبارات المستخدمة. ذلك أن تحديد مرامي العبارات وتحري مطابقة الألفاظ للمعنى الذي انتهى إليه الحكم وتسميتها باسمها المعين في القانون وتحديد ما إذا كانت سبًا أم قذفًا أم عيبًا أم إهانة أم تشهيرًا، هو من مسائل القانون التي يخضع فيه ما ينتهي إليه قاضي الموضوع لرقابة محكمة النقض[1]. ومثل هذا الأمر يتوافق مع وسيلة إثبات القصد الجنائي في هذه الجرائم، حيث يلزم لإثباته والتحقق من قيامه أن تكون الألفاظ

(1) طعن جنائي مصري رقم 3087 لسنة 62ق، جلسة 8/ 5/ 2000 (المحاماة/ مصر العدد 1 لسنة 2001، ص207).

المستخدمة في السب والقذف والتشهير شائنة بذاتها[1]، وتبتعد عن مدلول مجرد النقد المباح الذي لا يتضمن المساس بشخص صاحب الأمر أو التشهير به أو الخطّ من كرامته[2]. إذ يصلح أن يكون مبنى التجريم هنا أن يكون ذلك باستخدام نطاق اسم يحتوي على عبارات غير أخلاقية، مثل Fuckmickey. multimania. com حتى أن تضمّن الموقع مجموعة صور لأفراد برزت فقط وجوههم[3].

## المبحث السادس:
## جريمة الملاحقة والإزعاج

الملاحقة والمطاردة عبر الإنترنت Cyberstalking تعني قيام عضو الإنترنت بمراسلة واتصال مستمر بعضو أو أعضاء آخرين بقصد إزعاجهم Harassing وتهديدهم Threatening ومضايقتهم وإقلاق راحتهم. ويُعد العنصر النسائي عبر الإنترنت الهدف الأكثر تفاعلاً مع جريمة المطاردة والإزعاج هنا. إلا أن ذلك لا يمنع من وجود صور وأشكال أخرى للمطاردة، كما هو الشأن في مطاردة الموظف العام[4]، وكذلك مطاردة الأطفال عبر بث الأفكار المعادية للأجانب من عنصرية وكراهية إلى غير ذلك من مظاهر وأشكال هذه الجريمة. ومن ذلك أيضًا ما هو مقرر من مظهر تقليدي لجريمة المطاردة حسبما هو مقرر في المادة (472 ـ عقوبات ليبي) التي تنص على أن «كل من تسبب في مضايقة

(1) طعن جنائي مصري رقم 4933 لسنة 62ق، جلسة 15/ 5/ 2000 (المحاماة/ مصر العدد 1 لسنة 2001، ص207).

(2) طعن جنائي مصري رقم 3087 لسنة 62ق، السابق.

(3) TGI Meaux, 3eme Ch, Correc. 19/11/2001 (Ste Eurodisney S. C. A. & autres c/ A. A.)
http://www.juriscom.net.

(4) Paul Cullen QC - Computer Crime, op. cit. at 217.

الغير أو إقلاقهم في محل عام أو مفتوح أو معروض للجمهور، أو ضايقهم أو أقلقهم باستعمال التليفون أو استعمله لأي سبب ذميم آخر يعاقب بالحبس مدة لا تجاوز شهرين أو بغرامة لا تجاوز عشرين ديناراً».

وإذا كانت الإنترنت تعتمد على حركة الاتصالات عمومًا، وكانت في مرحلة زمنية تعتمد على خطوط الهاتف العادية، فإنه مع ذلك لا يمكن القول بامتداد مثل هذا النص للانطباق على الجرائم المرتكبة عبرها، لكون الإنترنت ليست هي الهاتف تحديدًا كما هو مقرر في النص المذكور، بالإضافة إلى كون الإنترنت تقنية تعتمد المعلوماتية، فهي هجين ناتج عن مزج هذا وذاك.

## أولاً: جريمة المطاردة في التشريع المقارن

في القانون الولائي الأمريكي يوجد حوالى ست عشرة ولاية قامت بسن تشريعات لمكافحة المطاردة عبر الإنترنت، ويكتفي بعض هذه التشريعات بوجود أي شكل من أشكال المطاردة، في حين يتطلب بعض هذه التشريعات قيام مرتكب الجريمة بإرسال تهديد حقيقي Transmit a credible threat للضحية أو عائلته أو أي شخص. وبعض الولايات الأخرى قامت بعدّ نطاق نصوص الاتصالات الهاتفية الفاحشة Obscene phone call بحيث تشمل عبارة Electronic communication device للاتصال بشخص وتهديده بارتكاب ضرر به أو بعائلته، مثل ولاية كاليفورنيا الأمريكية التي تعد من أوائل الولايات (الدول) التي قامت بسن تشريع يعاقب على ارتكاب جريمة المطاردة Cal. Penal code sec. 646. 9، وتلاها سبع ولايات هي -Alaska-Connecticut-Delaware Michigan-Montana-Oklahoma&Wyoming. ومن التشريعات الولائية الحديثة التي تأخذ بتقرير جريمة المطاردة عبر الإنترنت تشريع ولاية أركنساس الأمريكية التي تجرم قيام أي شخص بغرض التخويف أو التهديد أو الإساءة بالقيام بمطاردة أي شخص باستخدام المراسلة أو البريد الإلكتروني أو أية وسائل

اتصالية حاسوبية، وتتضمن هذه المراسلات التهديد بارتكاب أضرار مادية أو عدوان على الملكية أو كانت تحتوي هذه المراسلات على أسلوب فاحش أو فاسق أو لغة مدنسة.

ويُعاقب التشريع الفيدرالي الأمريكي على المطاردة عبر الإنترنت، فقد أدين Jack Backe، وهو طالب جامعي، بمقتضى نص القسم US Code Tit. 18 Sec. 875 ©، كونه في تاريخ سابق استخدم البريد الإلكتروني والمجموعة الإخبارية لبث قصة خطف وقتل شخص ما، ويلزم المحكمة وفق النص السالف أن يثبت لديها ثلاثة عناصر أساسية حتى يمكن الجزم بوقوع الجريمة وهي القيام بالتداول Transmission بين الولايات وأن يكون هناك اتصال يتضمن التهديد وأن يكون التهديد بقصد إحداث ضرر أو خطف لشخص آخر. كما يُعاقب التشريع الفيدرالي الأمريكي على مطاردة الرئيس الأمريكي إذا اقترنت هذه المطاردة بتهديد ما US Code Tit. 18 Sec. 871 بأية وسيلة اتصال مكتوبة أو مقروءة أو مسموعة ورقية أو مطبوعة أو رسالة أو وثيقة مادامت تحمل في مضمونها تهديدًا ما، وإن كان يشترط في جريمة مطاردة الرئيس الأمريكي أن تكون أحد أفعال المطاردة كالتهديد أو غيره ذات خصوصية صادرة عن الجاني وموجهة إلى الرئيس الأمريكي دون تلك الإشارات العامة.

وتعد جريمة التهديد من أشهر جرائم المطاردة عمومًا، والتهديد من الجرائم الشكلية التي لا يستلزم فيها حدوث نتيجة محددة، إذ يكفي فيها مجرد ارتكاب النشاط المادي تحديدًا، وليس الركن المادي كلية، وفي هذه الحالة يقوم التهديد كجريمة ويستحق مرتكبها العقاب. ويُعاقب القانون الولائي الأمريكي على التهديد كجريمة شكلية، فإكراه شخص على المكوث في المنزل، يعد من جرائم التهديد. كما أن القيام بتهديد شخص باستخدام رموز توحي بأن عدوانًا محتمل الحدوث ضده، يعد جريمة تهديد، كما لو قرر شخص أنه ينتمي إلى .P.D.L حال وجود خصام فوري مع آخر، فإن هذا يشكل

جريمة تهديد، دون لزوم معرفة طبيعة مثل هذه الكلمات، وما تعني كمختصرات، طالما أن الواقعة اتفقت مع الخصومة القائمة، مادام قد ترتب على الواقعة إدخال الرعب والخشية من وقوع جريمة على المجني عليه.

أما في القانون الإنجليزي، فيعدّ قانون الاتصالات لسنة 1984 هو القانون الذي يحكم واقعة المطاردة، حيث يعاقب القسم (43) منه على استخدام نظام اتصال عمومي A public telecommunications system لإرسال تهديد Threat أو مواد فحش Obscene أو مضرة Offensive، ويستشعر البعض من الفقه الإنجليزي كفاية هذا النص لانطباقه على البيانات Data التي ترسل عبر الإنترنت. وإن كان يرى أن في قانون الحماية ضد الإزعاج لسنة 1997 ما يكمل القانون الأول المشار إليه.

## ثانيًا: تحديد نشاط المطاردة

إن مصطلح المطاردة الجديدة التي لم يكن القانون الأنجلوفوني يعترف بها، ولقد كان السبب الرئيسي في بروز هذا المصطلح، هو التحرش الذي يصل في أغلب الأحيان إلى ارتكاب جرائم. والمصدر الأساسي لإقرار هذا النوع من العدوان هو موضوع المعاكسات التي يتعرض لها المجني عليه في هذه الجريمة. والواقع أن سلوك المطاردة يحمل على مفهوم القيام بمجموعة أفعال Course of Conduct [1] أو أنشطة تقوم على أساس فكرة الخوف من أفعال تجعل المجني عليه يعتقد اعتقادًا جازمًا بأنه عرضة لنتائج إجرامية من نوع ما. فهي تُحمل على مفهوم التهديد، كما تُحمل أيضًا على مفهوم الترهيب. دون اعتداد هنا بنية الجاني وفيما إذا كان يهدف بعمله هذا إلى القيام بما هو مشروع. وسلوك المطاردة عبر الإنترنت يجد له متسعًا، إذ يمكن باستخدام البريد الإلكتروني القيام بمراسلة شخص ما، واستمرار مراسلته بهدف تخويفه أو تهديده. ويجب

(1) Sec. 4 of the 1997 act (England).

أن يرتكب الجاني فعل المطاردة مرتين على الأقل لكي يمكن القول بتوافر الركن المادي كاملاً في هذه الجريمة[1]، وذلك ما يجعل هذه الجريمة تختلف عن التهديد الذي يحمل على كفاية ارتكاب التهديد ولو لمرة واحدة. وعليه فقيام عضو الإنترنت بمطاردة شخص آخر في حلقات النقاش بما يترتب على هذا النشاط تسبيب إزعاجٍ وخوفٍ في نفس المجني عليه هنا، يمكن أن يكون مثل هذا النشاط مرتبًا لجريمة مطاردة.

والحقيقة أن في مثل هذه الجريمة، ذات الطابع الجديد، يمكن القول بوجود جذور لها في القانون الليبي، كما هو الحال في المادة (359 ـ عقوبات ليبي) حيث' جاء في هذه المادة نشاط التتبع الذي يُحمَل بالتأكيد على مفهوم المطاردة حيث اعتبر المشرع الليبي هذا التتبع من التدابير غير المشروعة[2]. وإن كان يحتاج مثل هذا النص الأخير إلى مواءمته مع تكنولوجيا المعلومات، إذ يكفي مصطلح التتبع هنا بشرط الاستمرار لكي يفي جريمة المطاردة حقها في القانون.

وما يترتب عليه من نشاط المطاردة يجب أن ينعكس في نفس المجني عليه بالضرورة، دونما أهمية لما إذا كان الجاني Stalker في العالم المادي أو الافتراضي Cyber Stalcker قد يرتكب جريمة ضد المجني عليه، فهذا الأخير يسمى مجنيًا عليه في القانون بمجرد تكرار ارتكاب المطاردة لمرتين فأكثر ولو

---

(1) Paul Cullen QC. Op. cit.

(2) تنص المادة (359 ـ عقوبات ليبي) على أنه «يعاقب بالحبس مدة لا تزيد على سنة وبغرامة لا تقل عن مائة دينار ولا تجاوز خمسمائة دينار أو بإحدى هاتين العقوبتين، كل من استعمل القوة أو العنف أو الإرهاب أو التهديد أو التدابير غير المشروعة، بقصد إرغام الغير على الامتناع عن العمل أو إرغام رب العمل على استخدام شخص ما أو منعه من ذلك. وتطبق العقوبة ذاتها إذا كان القصد منع أي شخص من الاشتراك بأية نقابة. ويطبق حكم هذه المادة وإن استعملت القوة أو العنف أو الإرهاب أو التدابير غير المشروعة مع زوجِ الشخص أو مع أولاده. وتعد من التدابير غير المشروعة الأفعال الآتية على الأخص: أولاً: منع الشخص المقصود من مزاولة عمله بإخفاء أدواته أو ملابسه أو أي شيء آخر مما يستعمله أو بأية طريقة أخرى. ثانيًا: تتبعه بطريقة مستمرة في غدوه ورواحه. ثالثًا: الوقوف موقف التهديد بالقرب من منزله أو بالقرب من أي مكان يقطنه أو يشتغل فيه.

على فترات مختلفة، فقد يقوم الجاني بمطاردة فتاة في حلقة نقاش أو بطرقة المراسلة الإلكترونية، ثم يقف نشاطه لبضعة أيام ثم بعد ذلك يكرر محاولته معها مرة أخرى، فهنا يتوافر نشاط المطاردة، ويتحقق الركن المادي في الجريمة.

ولا يشترط القانون نشاطاً موحداً للمطاردة، إذ يمكن أن تقع هذه الجريمة باستخدام سلوك واحد بشكل متكرر، كما هو الشأن في التتبع المستمر المقرر في القانون الليبي، أو أن يقع بأكثر من شكل، كما لو قام الجاني بمطاردة شخص آخر في حلقة نقاش ثم بعد ذلك يتولى مطاردته باستخدام البريد الإلكتروني أو بمراسلته عبر قاعدة بيانات سجل الزيارات في الصفحة الخاصة به على موقعه عبر الإنترنت. كذلك لا يشترط أن يكون المظهر الإجرامي واضحاً في سلوك الجاني، بل يكفي ـ في رأينا ـ أن يكون مسلك الجاني لا يتضمّن نيّاتٍ إجرامية، فأسلوب الحث على استمرار الحديث عبر حلقة نقاش مع شخص محدد ربما يكون ظاهرًا منه حسن النية، ومع ذلك يكفي مجرد القيام بهذا النشاط للقول بتوافر الجريمة. ففي مثل هذه الحالة يكفي أن يكون المجني عليه غير مطمئن لاستمرار هذا الشخص في النقاش معه. فإذا استمر الجاني في تتبع المجني عليه من غرفة إلى أخرى ففي هذه الحالة تتوافر المطاردة، شريطة أن يكون المجني عليه قد أعلن له صراحة أو ضمنًا ممانعته في استمرار النقاش معه، أو مطالبته عبر البريد الإلكتروني بالكفّ عن مراسلته.

ويكفي للقول بتوافر الممانعة الضمنية ألا يقوم المجني عليه بالرد على مراسلات الجاني في الوقت الذي يستمر فيه الجاني في المراسلة مطالبًا المجني عليه بالرد أو بإيجاب طلباته. ولا يعد من هذا القبيل قيام الجاني بالتحرش بالمجني عليه، فتلك جريمة أخرى هي جريمة التحرش وهي من الجرائم الأخلاقية. وليس للجاني الاحتجاج يكون المجني عليه لم يعلمه صراحة برغبته في عدم التواصل معه، لكون هذه الجريمة من الجرائم التي تمثل عدوانًا على الحس الأخلاقي الإنساني الذي يجب أن يكون لدى كل إنسان.

## الفصل السادس

# الترتيبات الإجرائية والتشريعية لجرائم الإنترنت والمعلوماتية ودور التعاون الدولي

يقتضي للمجتمع المعلوماتي في مجال قانون الاجراءات الجنائية أن ينشئ قواعد قانونية حديثة بحيث توضع معلومات معينة تحت تصرف السلطة المهيمنة على التحقيق في مجال جرائم الكمبيوتر.

ومبّرر ذلك أن محترفي انتهاك شبكات الحاسبات الآلية ومرتكبي الجرائم الاقتصادية، وتجار الأسلحة والمواد المخدرة، يقومون بتخزين معلوماتهم في أنظمة تقنية المعلومات وعلى نحو متطور. وغالباً ما تصطدم الأجهزة المكلفة بالتحقيق بهذا التكنيك لتخزين المعلومات فيما هي تسعى جاهدة للحصول على أدلة الإثبات.

كما تصادف تلك الأجهزة الصعوبات عندما يتعلق الأمر، على وجه الخصوص، بتخزين بيانات في الخارج بوساطة شبكة الاتصالات البعدية[1]

(1) وعلاوة على ذلك فإن غالبية الإجراءات الجنائية لا تكون كافية ولا مناسبة لأغراض التحقيق والحكم في هذا النمط من أنماط الجرائم. لذا يبدو من الضروري إيجاد اجراءات لديها القدرة على الملاءمة مع المتطلبات الحديثة التي تفرضها تكنولوجيا المعلومات. راجع في ذلك : La criminamite informatique sur l'internet.

ويصعب حتى هذه اللحظة في غالبية الأنظمة القانونية أن نحدد إلى أي مدى تكفي الأساليب التقليدية للإكراه في قانون الإجراءات الجنائية من أجل مباشرة تحقيقات ناجحة في مجال تقنية المعلومات، لا سيما أنه اقترن بظهور تقنية المعلومات مشاكل خاصة ومستحدثة.

وعلى سبيل المثال التفتيش والتحفظ على المعلومات وإلزام المشاهد باسترجاع وكتابة المعلومات، والحق في مراقبة وتسجيل البيانات المنقولة بوساطة أنظمة الاتصالات البُعدية وجمعها وتخزينها وضم المعلومات الإسمية إلى الدعوى الجنائية.

ونظراً لسهولة حركة المعلومات في مجال أنظمة تقنية المعلومات، حيث تتيح هذه السهولة لحركة المعلومات إمكانية ارتكاب جريمة عن طريق حاسب آلي موجود في دولة معينة، بينما يتحقق نتيجة هذا، الفعلُ الإجرامي في دولة أخرى.

لذا يقتضي الأمر ضرورة وجود تعاون دولي مُحْكَم في مجال مكافحة هذا النوع من الجرائم، وأيضاً لأجل توفير حماية حقيقية لأنظمة الاتصالات البُعدية.

على أية حال ينقسم هذا الفصل إلى ثلاثة مباحث، اختصّ المبحث الأول منها بمعالجة إجراءات جمع الأدلة فيما يتعلّق بجريمة سرقة المعلومات، في حين تناول الثاني معوقات جمع الأدلة في مجال جريمة سرقة المعلومات. أما الثالث فقد ركّز على بيان دور التعاون الدولي في مجال مكافحة الجريمة المعلوماتية

## المبحث الأول:
## معالجة إجراءات جمع الأدلة بخصوص جريمة سرقة المعلومات

مبدئياً؛ إجراءات التحقيق هي مجموعة الأعمال التي يرى المحقق وجوب، أو ملاءمة القيام بها لكشف الحقيقة بالنسبة لواقعة معينة يهتم بها قانون العقوبات.

وتنقسم هذه الإجراءات إلى قسمين: أحدهما يسعى للحصول على الدليل، كالتفتيش وسماع الشهود، والثاني يمهّد للدليل ويؤدي إليه، كالقبض والحبس الاحتياطي.

وتسمى المجوعة الأولى : إجراءات جمع الأدلة، أما الثانية: فتعرف بالإجراءات الاحتياطية ضد المتهم.

وسوف تقتصر دراستنا على الإجراءات الخاصة بجمع الأدلة، وهذه إجراءات تنطوي أيضاً على المساس بالحريات وهذا أبرز ما يميزها، ولهذا فإنه يجب النظر اليها باعتبارها واردةً على سبيل الحَصْر، فلا يجوز للمحقق أن يباشر إجراءً آخر فيه مساس بحريات الأفراد ولو كان من شأنه أن يؤدى إلى كشف الحقيقة، كاستعمال جهاز كشف الكذب أو مَصْل الحقيقة.

وإجراءات جمع الأدلة، كما حدّدها القانون، هي : المعاينة، نَدْب الخبراء، التفتيش، وضبط الأشياء ومراقبة المحادثات وتسجيلها وسماع الشهود والاستجواب والمواجهة.

وليس على المحقق الالتزام باتباع ترتيب معين عند مباشرة هذه الإجراءات بل هو غير ملزم أساساً لمباشرتها جميعاً، وأنما يباشر منها ما تمليه مصلحة التحقيق وظروفه ويرتّبها وفقاً لما تقضي به هذه المصلحة وما تسمح به هذه الظروف.

## معاينة مسرح الجريمة والمعلوماتية

يقصد بالمعاينة فَحصُ مكان أو شيءٍ أو شخص له علاقة بالجريمة وإثبات حالته[1]، كمعاينة مكان ارتكاب الجريمة أو أداة ارتكابها أو محلها أو معاينة

(1) توجب المادة 35 من قانون الإجراءات الجزائية الإماراتي، على مأموري الضبط القضائي وعلى مرؤوسيهم، إجراء المعاينة اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم أو التي يعملون بها بأية كيفية كانت. وتقضي المادة 43 من القانون ذاته أنه على مأمور الضبط القضائي في حالة التلبس =

جسم أو ملابس الجاني أو المجني عليه لإثبات ما بالجسم من جراح وما على الثياب من دماء أو ما بها من مزق أو ثقوب.

ويلاحظ أن المعاينة قد تكون إجراء تحقيق أو استدلال، ولا تتوقف طبيعتها على صفة من يجريها بل على مدى ما يقتضيه إجراؤها من مساس بحقوق الأفراد، فإذا جرت المعاينة في مكان عام كانت إجراءَ استدلالٍ، وإذا اقتضت دخول مسكن أو له حرمة خاصة كانت إجراءً تحقيق[1].

والمعاينة جوازية للمحقق شأنها شأن سائر إجراءات التحقيق فهى متروكة الى تقديرة سواء طلبها الخصوم أو لم يطلبوها ولا تتمتع المعاينة في مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية[2]. ومرد ذلك في اعتبارين :

الأول: أن الجرائم التي تقع على نظم المعلومات والشبكات قلّما يترتب على ارتكابها آثار مادية.

الثاني: أن عدداً كبيراً من الأشخاص قد يتردد على مكان أو مسرح الجريمة خلال الفترة الزمنية التي تتوسط عادة ارتكابها الجريمة واكتشافها مما

---

= بجريمة أن ينتقل فوراً لمحل الواقعة ويعاين الأثار المادية للجريمة ويحافظ عليها ويثبت حالة الأماكن والأشخاص وكل ما يفيد في كشف التحقيق. . وعليه إخطار النيابة العامة فوراً بانتقاله، وعلى النيابة العامة الانتقال فوراً إلى محل الواقعة بمجرد إخطارها بجناية متلبَّس بها.
كما تنص المادة 90 من قانون الإجراءات الجنائية المصري على أن ينتقل قاضي التحقيق إلى أي مكان كلما ارتأى ذلك ليثبت حالة الأمكنة والأشياء والأشخاص ووجود الجريمة مادياً وكل ما يلزم إثبات حالته. أو المقصود بهذا النص تيسير مهمة المحقق وتمكينه من إنجاز التحقيق بالسرعة اللازمة قبل أن تندثر معالم الجريمة أو تطمس أدلتها فيتعذر الوصول إلى الحقيقة بعد ذلك.

(1) انظر في ذلك : د. عوض محمد ـ قانون الإجراءات الجنائية ـ الجزء الأول 1989 مؤسسة الثقافة الجامعية ص470 وما بعدها.

(2) انظر في ذلك أيضاً د. محمد محمد عنب، معاينة مسرح الجريمة ـ رسالة دكتوراه أكاديمية الشرطة ـ كلية الدراسات العليا القاهرة ـ 1988، ص13، وما بعدها.

يهيئ الفرصة لحدوث تغيير أو إتلاف أو عبث بالآثار المادية[1]، أو زوال بعضها وهو ما يثير الشك في الدليل المستمد من المعاينة، وحتى تصبح معاينة مسرح الجريمة المعلوماتية لها فائدة في كشف الحقيقة عنها وعن مرتكبها فإنه ينبغي مراعاة عدة قواعد وإرشادات فنية أبرزها ما يلي:

1 ـ تصوير الحاسب والأجهزة الطرفية المتصلة به، والمحتويات والأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب وملحقاته، ويراعى تسجيل وقت وتاريخ ومكان التقاط كل صورة.

2 ـ العناية البالغة بملاحظة الطريقة التي تمّ بها إعداد النظام والآثار الإلكترونية وبوجه خاص السجلات الالكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي جرى عن طريقه الولوج إلى النظام أو الموقع أو الدخول معه في حوار.

3 ـ ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل حين عرض الأمر فيما بعد على القضاء.

4 ـ عدم نقل أية مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد

---

(1) تنص المادة 266 عقوبات اتحادي فتقضي بأن يعاقب بالحبس كل من غيّر بقصد تضليل القضاة حالة الأشخاص أو الأماكن أو الأشياء أو أخفى آلة الجريمة أو قدم معلومات كاذبة تتعلق بها وهو يعلم عدم صحتها. كما تنص المـادة 286 من القانون ذاتـه على أن من أخفى أو آوى بنفسه أو عَبْر غيره شخصاً في بيته قبل القبض عليه أو متهماً في جريمة أو صادرا في حقه أمر بالقبض عليه، وكذلك كل من أعانه بأية طريقة كانت على الفرار من وجه العدالة مع علمه بذلك يعاقب طبقا للأحوال الآتية.. «وتقضي المادة 287 من ذات القانون أيضاً بأن من علم بوقوع جريمة وأعان مرتكبيها على الفرار من وجه العدالة بإخفاء دليل من أدلة الجريمة... أو أعانه بأية طريقة أخرى يعاقب طبقاً للأحوال الأتية.. «كما تنص المادة 145 عقوبات مصري على أنه كل من علم بوقوع جناية أو جنحة أو كان لديه ما يحمل على الاعتقاد بوقوعها وأعان الجاني بأية طريقة كانت على الفرار من وجه القضاء إما بإيواء الجاني المذكور وإما بإخفاء أدلة الجريمة أو بتقديم معلومات تتعلق بالجريمة وهو يعلم بعدم صحتها أو كان لديه ما يحمله على الاعتقاد بذلك يعاقب.. ».

من خلوّ المحيط الخارجى لموقع الحاسب من أية مجالات لقوى مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة.

5 ـ التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة أو المحطّمة وفحصها، ورفع البصمات التي قد تكون لها صله بالجريمة المرتكبة.

6 ـ التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليه من بصمات[1].

7 ـ إعداد خطة الهجوم بحيث تكون الخطة واضحة ومفهومة لدى أعضاء الفريق، على أن تكون الخطة موضحة بالرسومات لتجري مراجعتها مع أعضاء الفريق قبل بدء التحرك، مع الأخذ في الاعتبار قاعدة smeac العسكرية والتي تعني الحالة (situation) الرسالة (mission) التنفيذ (execution) المداخل والمخارج (avenues of approach) والاتصالات (communication) وهي ملائمة للأجهزة الأمنية أحهزة تنفيذ القوانين، فالحالة أو الوضع يعني معرفة حجم القضية التي تقوم بالتحقيق فيها، وعدد المتورطين فيها. أما الرسالة فهى تحديد الهدف من الغارة، والتنفيذ يعنى كيفية أداء المهمة، أما المداخل والمخارج فإن معرفتها ضرورية وهي تختلف من جريمة لأخرى وتحسب وفقاً لمكونات طريق التحقيق، بينما يأتي عنصر الاتصالات لضمان السرية وسلامة التعامل وتبادل المعلومات أثناء عملية الغارة.

وبعد وصول الفريق إلى مسرح الجريمة أو مكان الغارة يتم التأمين والسيطرة على المكان والبدء في التفتيش على النحو التالي :

---

(1) راجع في ذلك : د. هشام محمد فريد رستم، سبقت الإشارة إليه، ص104 وما بعدها.

أ - السيطرة على المناطق المحيطة بمسرح الجريمة أو مكان الإغارة، وذلك عن طريق إغلاق الطرق والمداخل.

ب - السيطرة على الدائرة المحيطة بمكان الإغارة بوضع حراسات كافية لمراقبة التحركات داخل الدائرة ورصد الاتصالات الهاتفية من وإلى مكان الإغارة مع إبطال أجهزة الهاتف النقال.

ج - تأمين موقع الغارة والسيطرة على جميع أركانها ومنافذها والتحفظ على الأشخاص الموجودين.

د - تحديد أجهزة الحاسب الآلي الموجودة في مكان الإغارة وتحديد مواقعها بأسرع فرصة ممكنة، وفى حالة وجود شبكة اتصالات يجب البحث عن خادم الملف file server لتعطيل حركة الاتصالات.

و - يوضع حرس على كل جهاز حتى لا يتمكن أحد المتهمين من إتلاف المعلومات من بُعْدٍ، أو من جهاز آخر داخل المبنى.

هـ - اختيار مكان لمقابلة المتهمين والشهود على أن يكون المكان بعيداً عن أجهزة الحاسب الآلي[1].

## التفتيش في مجال الجريمة المعلوماتية

التفتيش في قانون الإجراءات هو البحث عن شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، وقد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة، وقد أحاط القانون هذا التفتيش بضمانات عديدة. ومحل التفتيش إما أن يكون مسكناً أو شخصاً، وهو بنوعَيْه قد يكون متعلقاً بالمتهم أو بغيره، وهو في كل أحواله جائز مع اختلاف في بعض الشروط[2].

(1) راجع في ذلك : د. محمد الأمين البشري؛ التحقيق في جرائم الحاسب الآلي بحث مقدم إلى مؤتمر القانون والإنترنت بتاريخ 3 مايو 2000 لجامعة الإمارات ص30.

(2) انظر في ذلك : د. عوض محمد، سبقت الإشارة إليه ص475.

## مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش

يتكون الحاسب الآلي من مكونات مادية Hard ware ومكونات منطقية soft ware: كما أن له شبكات اتصالات بُعْدية سلكية ولا سلكية سواء على المستوى المحلي أو المستوى الدولي فهل تخضع هذه المكونات للتفتيش؟

### أولاً: مدى خضوع مكونات الحاسب المادية للتفتيش:

يخضع الولوج في المكونات المادية للحاسب بحثاً عن شيء يتصل بجريمة معلوماتية وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها للإجراءات القانونية الخاصه بالتفتيش. وبعبارة أخرى فإن جواز تفتيش تلك المكونات يتوقف على طبيعة المكان الحاصل فيه التفتيش، وهل هو مكان عام أم مكان خاص. إذ إن لصفة المكان أهمية خاصه في مجال التفتيش؛ فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته، كان لها حُكْمُه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبالضمانات نفسها المقررة قانوناً في محنلف التشريعات.

ويجب التمييز داخل المكان الخاص بين ما إذا كانت مكونات الحاسب منعزلة عن غيرها من الحاسبات الأخرى أم أنها متصله بحاسب أو بنهاية طرفية terminal في مكان آخر، كمسكن لا يخص مسكن المتهم. فإذا كانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة، تعيّن مراعاة القيود والضمانات التي يستلزمها المشرّع لتفتيش هذه الأماكن. أما بالنسبة للأماكن العامة، فإذا وجد شخص وهو يحمل مكونات الحاسب الآلي المادية أو كان مسيطراً عليها أو حائزاً لها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص بالضمانات والقيود نفسها المنصوص عليها في هذا المجال.

ومن التشريعات التي تجيز تفتيش مكونات الحاسب الآلي نذكر المادة 251

من قانون الإجراءات الجنائية اليوناني[1]، والمادة 487 من قانون الإجراءات الكندي [2]. وهناك قله من التشريعات تنص صراحة على تفتيش مكونات الحاسب الآلي، من ذلك القانون الانجليزى السابق سنة 1990 والذى يطلق عليه قانون إساءة استخدام الحاسب computer misuse [3]، كذلك هناك بعض القوانين التي تحتوي على قواعد تفصيلية للتفتيش تطبق على مكونات الحاسب وبياناته في حالات معينة. ومن ذلك على سبيل المثال القسم رقم 16 ـ 1 من قانون المنافسة competition في كندا حيث يمنح الشخص .A.C.T الذى يحمل إذناً بالتفتيش الحقّ في أن يستخدم أي نظام للحاسب الآلي لتفتيش أي بيانات يحتويها أو تكون متاحه لهذا النظام أو يجوز له أن يسجل أو يعمل على تسجيل تلك البيانات في شكل مطبوعات، أي مخرجات أخرى[4].

**ثانياً: مدى خضوع مكونات الحاسب المعنوية للتفتيش:**

بالنسبة لتفتيش مكونات الحاسب المعنوية فقد ثار الخلاف بشأن جواز تفتيشها، حيث يذهب رأيٌ إلى أنه اذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة. فإن هذا المفهوم يمتد ليشمل البيانات الإلكترونية بمختلف أشكالها. وفي هذا المعنى نجد المادة 251 من قانون الإجراءات الجنائي اليوناني تعطي سلطات التحقيق إمكانية القيام (بأي شيء

(1) Vassilaki (Irini): computer crimes and other crimes against information technology in Greece RI.D.P. 1993,P.371

مُشار إليه: د. هلالي عبد الله أحمد، تفتيش الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة 1997، ص74.

(2) pirgoff (Donoldk): computer crimes and other crimes against information technology in Canada R.I.D.P. 1993,P.241

(3) ferbrache (david): Pathology of computer viruses springer verly London L.T.D. 1992,P.233

(4) DURAM (COLO): The emerging strucrues of criminal information law tracing the contours of a new poraigm R.I.D.P.1993,P.111

يكون ضرورياً لجمع وحماية الدليل). ويفسر الفقه اليوناني عبارة «أي شيء» بأنها تشمل ضبط البيانات المخزنة أو المعالجة الكترونياً. ولذلك فإن ضبط البيانات المخزنة في الذاكرة الداخلية للحاسب الآلي لا تشكل أية مشكلة في اليونان، إذ بمقدور المحقق أن يعطى أمراً للخبير بجمع البيانات التي يمكن أن تكون مقبوله كدليل في المحاكمة الجنائية[1].

وتمنح المادة 487 من القانون الجنائي الكندي سلطة اصدار إذن لضبط أي شيء طالما تتوافر أسس معقولة للإعتقاد بأن الجريمة ارتكبت أو يشتبه في ارتكابها أو أن هناك نية في أن يستخدم في ارتكاب الجريمة أو أنه سوف ينتج دليلاً على وقوع الجريمة.

وهكذا يفسِّر هذا النص بوضوح على أنه يسمح بضبط بيانات الحاسب غير المحسوسه[2]. وهناك على النقيض رأي أخر يرى أنه إذا كانت الغاية من التفتيش هى ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن هذا المفهوم المادي لا ينطبق على بيانات الحاسب الآلي غير المحسوسة أو الملموسة.

ويقترح هذا الرأي، في مواجهة هذا القصور التشريعي، ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش عبارة (المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي) وبذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني الحديث هي (البحث عن الأدلة المادية أو أي مادة معالجة بوساطة الحاسب)[3].

ويرى بعض الفقهاء في فرنسا أن النبضات الإلكترونية Electronic Im-pulse أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة،

---

(1) راجع في ذلك : د. هلالي عبد اللاه أحمد، سبقت الإشارة إليه ص 82.
(2) راجع في ذلك : د. هلالي عبد اللاه أحمد، سبقت الإشارة إليه ص 83.
(3) انظر في ذلك : د. هلالي عبد اللاه أحمد، سبقت الإشارة إليه ص 84.

وتالياً لا تعتبر شيئاً مادياً بالمعنى المألوف للمصطلح[1]. ولذا لا يمكن ضبطها.

وفى الولايات المتحدة الأمريكية تم تعديل القاعدة رقم 34 من القواعد الفيدراليه الخاصة بالإجراءات الجنائية عام 1970 لتنص على السماح بتفتيش أجهزة الكمبيوتر والكشف عن الوسائط الإلكترونية بما في ذلك البريد الإلكترونى والبريد الصوتي والبريد المنقول وعن طريق الفاكس[2].

وتتركز أذون التفتيش القياسية الصادرة عند التفتيش في إحدى جرائم الكمبيوتر، وبصفة خاصة، على ضبط الوثائق المكتوبة فضلاً عن أجهزة الكمبيوتر وتتضمن هذه الوثائق على وجه التحديد: النسخ الضوئية، مطبوعات الكمبيوتر، فواتير التليفون، سجلات العناوين، والمذكرات والمراسلات[3].

### ثالثاً: مدى خضوع شبكات الحاسب للتفتيش:

ويمكن في الفرض التمييز بين ثلاثة احتمالات:

الاحتمال الأول: اتصال حاسب المتهم بحاسبٍ أو نهاية طرفية موجودة في مكان آخر داخل الدولة: ويرى الفقه الألماني بشأن مدى إمكانية امتداد الحق في التفتيش اذا تبين أن الحاسب أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو طرفية في مكان آخر مملوك لشخص غير المتهم، أنه يمكن أن يمتد التفتيش في هذه الحالة إلى سجلات البيانات التي تكون في موقع آخر استناداً إلى مقتضيات القسم 103 من قانون الإجراءات الجنائية الألماني [4].

---

(1) انظر في ذلك: Linformatique. J.c.P. 1989 3333 no. 16
Gassin (R) le droit penal et linformatiqe D.1982.p.38

(2) راجع في ذلك: Linda volonino ibid, p.2

(3) انظر في ذلك: Brucisterling, ibid, p. 165

(4) KASPERSEN (W.K. Henrik): computer crimes and other crimes against information technology in the Netherlands R.I.D.P.1993,P.479

كما نصّ مشروع قانون جرائم الحاسب الآلي في هولندا[1] على جواز أن يمتد التفتيش إلى نظم المعلومات الموجودة في موقع آخر بشرط أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة (القسم الخامس من المادة125) وذلك بمراعاة بعض القيود.

الاحتمال الثاني: اتصال حاسب المتهم بحاسب أو نهاية طرفية موجودة في مكان أخر خارج الدولة : من المتصوّر طبقاً لهذا الاحتمال أن يقوم مرتكبو الجرائم بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الدولة، عن طريق شبكات الاتصالات البُعُدية بهدف عرقلة سلطات الادعاء في جَمْع الأدلة. ولمواجهة هذا الاحتمال نصّ مشروع قانون جريمة الحاسب الآلي بهولندا أنه يجوز لجهات التحقيق مباشرة التفتيش داخل الأماكن، وبما ينطوي عليه تفتيش نظم الحاسب المرتبطه، حتى إذا كانت موجودة في دول أخرى، وبشرط أن يكون هذا التدخل مؤقتاً وأن تكون البيانات التي يتم التفتيش عنها لازمة لإظهار الحقيقة (المادة 125)[2].

ووفقاً لما جاء في تقرير المجلس الأوروبي فإن هذا الاختراق المباشر يعتبر إنتهاكاً لسيادة دولة أخرى ما لم توجد اتفاقية دولية في هذا الشأن، ويؤيد الفقه الإلماني ما جاء في تقرير المجلس الأوروبي حيث أن السماح باسترجاع البيانات التي تم تخزينها في الخارج يعتبر انتهاكاً لحقوق السيادة لدولة أخرى وخرقاً للقوانين الثنائية والوطنية الخاصة بإمكانية التعاون في مجال العدالة القضائيه[3]. وقد أيد القضاء الألماني هذا الاتجاه حيث أسفر البحث في إحدى

---

(1) راجع في ذلك : د. هلالي عبد اللاه أحمد، سبقت الإشارة إليه ص 77.

(2) DURHAM (COLO): the emerging structures of criminal infromatin law: tracing the contours of a new paradigm general report for the a.i.d.p. collwuium R.I.D.P. 1993.P.115

(3) راجع في ذلك:
Mohrenschl ager (Mnfred): computer crimes and other crimes against information technology in Germany r.i.d.p.1993,p.351

جرائم الغش المعلوماتي عن وجود طرفية حاسب في ألمانيا متصلة بشبكة اتصالات في سويسرا حيث يتم تخزين بيانات المشروعات فيها، وعندما أرادت سلطات التحقيق الألمانية الحصول على هذه البيانات لم يتحقق لها ذلك إلا من خلال طلب المساعدة المتبادلة request for mutual assistance [1]. وقد ساور الاعتقادُ الشرطةَ اليابانية بأن مجموعة من المخربين قد استخدمت أجهزة الكمبيوتر في الصين والولايات المتحدة في مهاجمة العديد من المواقع الخاصة للحكومة اليابانية على الشبكة، وقد طالبت الشرطة اليابانية كلاً من بكين وواشنطن بتسليم بيانات الدخول المسجلة على أجهزة الكمبيوتر في كل من هاتين الدولتين حتى يتمكنوا من الوصول إلى جذور هذه العملية الارهابية[2]

الاحتمال الثالث: يسمح بالتنصّت WIREAPPING والأشكال الأخرى للمراقبة التليفونية في العديد من الدول[3]، حيث يجيز القانون الفرنسي الصادر في 10 يوليو/ تموز سنة 1991 لاعتراض الاتصالات البُعْدية (telem atiqe) بما في ذلك شبكات تبادل المعلومات[4]. ويجوز لقاضي التحقيق في هولندا أن يأمر بالتنصّت على شبكات اتصالات الحاسب اذا كانت هناك جرائم خطيرة متورط فيها المتهم، وتشمل هذه الشبكة التلكس والفاكس ونقل البيانات Data communication [5]. وفي الولايات المتحدة الأمريكية ـ يجوز اعتراض الاتصالات الإلكترونية بما فيها شبكات الحاسب بشرط الحصول على إذن تفتيش صادر من القاضي [6].

---

(1) ibid.p. 365.

(2) راجع في ذلك : Linda volonio ibid., p.4.

(3) راجع في ذلك : DURHAM (COLO) op.cit., p. 113

(4) راجع في ذلك : Dr: Jacques francillon. op.cit. 304

(5) KASPERSEN (W.K.Henrik): Computer crimes and other crimes against information technology in the nether lands r.i.d. p. 1993,p.500

(6) راجع في ذلك : BRUCITERLING ibid, p. 165

## ضوابط تفتيش نظم الحاسب الآلي

يمكن تقسيم ضوابط تفتيش نظم الحاسب الآلي إلى نوعين : الأولى موضوعية، والأخرى: شكلية.

### أولاً : الضوابط الموضوعية لتفتيش نظم الحاسب الآلي :

وتنحصر هذه الضوابط في :

أ ـ وقوع جريمة معلوماتية: والجريمة المعلوماتية هى كما سبق القول؛ كلّ فعل غير مشروع مرتبط باستخدام الحاسب الآلي لتحقيق أغراض غير مشروعة[1] .

وهناك العديد من التشريعات التي حرصت على استحداث نص خاص للجريمة المعلوماتية كما هو الحال بالنسبة لإنجلترا، والتي أصدرت قانون اساءة استخدام الحاسب الآلي computer misuse act في 29 يونيو/ حزيران 1990[2] . وفي الولايات المتحدة الأمريكية حيث صدر قانون

---

(1) انظر في ذلك : د. محمد سامي الشواء، سبقت الإشارة إليه، ص. 8.
د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، ص30

(2) this act made it acriminal offence for anyone to acces of to modify computer held data or software without authority, or attempt to do so.
It created three specific offenceses.
1 - Accessis delibnerate and unothorieses.
2 - Access is without authority and with attention to commit afurther offense (either immediately or in the future).
3 - A person does and eliberte act that causes and unaut horises modification of the computers content

وهناك عدة ملاحظات على نصوص هذا القانون وهي :
ـ إن التآمر والشروع والتحريض تعد جميعها من بين الجرائم.
ـ لا يُلزَمُ الادعاء بالحصول على دليل يفيد بأن تلك الأفعال قد تم توجيهها صوب بنود معينة من البيانات أو البرامج.
ـ لا يُلزم وجود المتهم في المملكة المتحدة وقت ارتكاب الجريمة.
ـ لا يلزم وجود بيانات الكمبيوتر المستهدفة في المملكة المتحدة.

الاحتيال واساءة استخدام الحاسب الآلي سنة 1986 والذي طبق على المستوى الفيدرالى[1]، بالاضافة إلى قوانين بعض الولايات الأمريكية كقانون ولاية تكساس الصادر في أول سبتمبر/أيلول سنة 1985 بشأن الدخول غير المشروع في نظام الحاسب وفي فرنسا صدر قانون رقم 19 ـ 88 في 5 يناير/ك2 1988 وهو الخاص بالغش المعلوماتي[2]، والذي تم تعديله مع صدور قانون العقوبات الفرنسي الجديد الذي بدأ العمل به اعتباراً من أول مارس/آذار 1994، وفي الدنمارك صدر قانون جرائم الحاسب في 6 يونيو/حزيران سنة 1985.

وقد أَدرج المشرّع الإماراتي برامج الحاسب ضمن المصنفات الفكرية المحمية بالقانون الاتحادي رقم 40 لسنة 1992، كذلك اعتبر المشرّع المصري مصنفات الحاسب الآلي من برامج وقواعد بيانات وما يماثلها من مصنفات، تحدد بقرار من وزير الثقافة ضمن المصنفات المشمولة بحماية حق المؤلف المنصوص عليها في المادة الثانية بمقتضى القانون رقم 38 لسنة 1992.

ب ـ تورّط شخص أو أشخاص معينين في ارتكاب الجريمة المعلوماتية أو الاشتراك فيها: ينبغى أن تتوافر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة المعلوماتية، سواءٌ بوصفه فاعلها أو شريكاً فيها؛ وفي مجال الحاسب الآلي يمكن القول بأن تعبير الدلائل الكافية يُقصد به مجموعة من المظاهر أو الأمارات المعنية التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة وكذلك

(1) راجع في ذلك:
Jackson (K.M.), HRUSKA (Op.cit.,passim.,pp.): Computer security refernce book editor donn B. Parker 1992,p.401

(2) راجع في ذلك:
Chamaux (Francais) la loi sur la fraude infromatique de nouvelles incriminations J.C.P. 1988-1-3321.

على خبرة وحرفية القائم بالتفتيش، والتي تؤيد نسبة الجريمة المعلوماتية إلى شخص سواء بوصفه فاعلاً أو شريكاً.

جـ ـ توافر أَماراتٍ قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم. ولا يقتضي التفتيش إلا إذا توافرت لدى المحقق أسباب كافية على أنه يوجد في مكانٍ، أو لدى الشخص المراد تفتيشه، أدوات استخدمت في الجريمة المعلوماتية أو أشياء متحصّلة منها، أو مستجدات الكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المتهم أو غيره، إذ من المقرر أن كلّ ما يُشترط لصحة التفتيش الذي تجريه النيابة أو تأذن في اجرائه في مسكن المتهم أو ما يتصل بشخصه، هو أن يكون رجل الضبط القضائي قد علم من تحرياته واستدلالاته أن جريمةً معينةً ـ جناية أو جنحة ـ قد وقعت من شخص معين، أو أن يكون هناك من الدلائل والأمارات الكافية والشبهات المقبولة ضد هذا الشخص بقدْرٍ يبرّر تعرض التفتيش لحريته أو لحرمة مسكنه في سبيل كشف اتصاله بالجريمة المعلوماتية[1].

د ـ ومحلّ التفتيش الخاص بنُظُم الحاسب الآلي هي كل مكونات الحاسب سواء كانت مادية أو معنوية أو شبكات الاتصال الخاصة به بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش.

وتشمل المكونات المادية للحاسب وحدة الإدخال Input ووحدة الذاكرة الرئيسية Main Memory ووحدة الحساب والمنطق Arithmatic and logic unit وحدات الاخراج Output وأخيرا وحدات التخزين الثانوية age Units Secondary.

كما تنقسم المكونات المعنوية للحاسب إلى الكيانات المنطقية الأساسية

(1) نقض، 26 يناير: ك2 سنة 1981 مجموعة أحكام النقض س 50 رقم 12 ص79.

أو برامج النظام والكيانات المنطقية التطبيقية، أو برامج التطبيقات بنوعيها، برامج التطبيقات سابقة التجهيز وبرامج التطبيقات طبقاً لاحتياجات العميل. ويستلزم الحاسب بمكوناته سالفة الذكر، مجموعة من الأشخاص لديهم خبرة ومهارة في تقنية نظم المعلومات، وهم مشغّلو الحاسب computer aperators وخبراء البرامج programmers سواء كانوا مخطّطي برامج تطبيقات أم كانوا مخطّطي برامج نظم، والمحللين ومهندسي الصيانة والاتصالات ومديري النظم المعلوماتية.

**ثانياً: الضوابط الشكلية لتفتيش نظم الحاسب الآلي:**

أ - الأسلوب الآلي لتنفيذ التفتيش في نظم الحاسب الآلي:

ب - نظّم القانون الأمريكي أسلوب تنفيذ التفتيش في نظم الحاسب الآلي وذلك على النحو التالي:

تقتحم قوات الشرطة المكان بصورة سريعة ومن منافذه كافة في آن واحد وذلك باستخدام القَدْر الأعظم من القوة، بافتراض أن هذا التكتيك يقلّل من احتمال وقوع إصابات بين صفوف رجال الشرطة.

يتم إبعاد سائر المشتبه فيهم عن جميع أنظمة ومعدات الكمبيوتر الموجود في المكان على الفور، حتى لا يتمكنوا من تشويه أو تدمير أي دليل الكتروني، ويتم إدخال سائر المشتبه فيهم إلى غرفة لا توجد فيها أية أجهزة كمبيوتر، ودائماً ما تكون غرفة المعيشة، ويوضعوا تحت حراسة مشددة، وفي هذه الخطوة يتم تقديم إذن التفتيش الصادر من النيابة إليهم ويتمّ تحذيرهم بأن أقوالهم كافة ستُحسب عليهم منذ هذه اللحظة وقد تؤخذ كدليل إدانة ضدهم، ودائماً ما سنجد لدى العديد منهم الكثير من الحديث، وبخاصة إذا ما كانوا أولياء أمور غافلين عن حقيقة ما يحدث في منازلهم. وفي مكان ما من المنزل، سنجد النقطة الساخنة ـ جهاز كمبيوتر متصل بخط تليفوني، أو ربما نجد أكثر من جهاز

وأكثر من خط في المنزل الواحد، وعادةً ما تكون هذه النقطة الساخنة داخل غرفة النوم الخاصة بأحد الأبناء المراهقين (أو في أيّ مكان آخر داخل المنزل).

توضع النقطة الساخنة في عهدة فريق يضم اثنين من العملاء، «مُكتشِف» و«مُسَجِّل»، ويجب أن يكون المكتِشف من بين العملاء الذين تمّ تدريبهم تدريباً متقدماً على نظم المعلومات، ودائماً ما يقوم بهذا الدور العميل المعنيّ بالقضية والذي عاصرها من البداية واستصدر إذن التفتيش الخاص بها من القاضي، فهذا الشخص يعرف تماماً الشيء أو الأشياء التي يبحث عنها ويتفهم طبيعتها تماماً، ولن نبالغ إذا ما قلنا أنه هو الذي يقوم بعملية الضبط. ويتولى المكتشف نزع مَقْبَس الكهرباء الخاص بسائر الأجهزة ويقوم بفتح الأدراج والبحث عن الديسكات والملفات وحاويات الأسطوانات. . . إلخ.

أما المُسجِّل فيتولى تصوير سائر الأجهزة والمعدات على الكيفية ذاتها التي تم ضبطُها عليها ـ وبخاصةٍ وصلات الأسلاك المتشابكة الملقاة خلف الأجهزة (حتى يتمكن الفريق من إعادة تجميعها مثلما كانت عليه).

ويقوم المسجل كذلك، عادةً، بتصوير جميع الغرف الأخرى الموجودة في المنزل حتى لا يدّعي أحد المجرمين الماكرين أن الشرطة قد سرقت منزله أثناء التفتيش، ويحمل بعض المسجلين كاميرات فيديو أو أجهزة تسجيل صوتي ويتمّ توصيف الأشياء، التي تم العثور عليها وترقيمها، ودائماً ما يتم ذلك على استمارة مطبوعة معممة الاستخدام في سائر أجهزة الشرطة[1].

ب ـ فريق التفتيش، وهو الفريق المعنيّ بإجراءات التحقيق والذي هو جزء داخل فريق الإغارة الذي يضم، بجانب فريق التفتيش والضبط، رجالَ الحراسات والأمن وقوات الحماية والتأمين ورجال المباحث والمراقبة السرية والمعاونين من العمال والعمّال المَهَرة والسائقين وخيراء مسرح

(1) انظر في ذلك : Brucistercing ibid,p.165

الجريمة العادية الملائمين للجريمة موضوع التحقيق. ويتكون فريق التفتيش والضبط من :

**المشرف على التحقيق:**

والمسؤول عن هذا الجزء يجب أن يكون من ذوي الخبرات الطويلة في مجال التحقيق الجنائي في الجرائم المعقدة، ويتولى المشرف إدارة العمل في مسرح الجريمة وتوزيع المهام على أعضاء الفريق.

**فريق أخذ الإفادات:**

ويُحدَّد عدد أعضاء هذا الفريق حسب حجم الجريمة والمتورطين فيها وعدد الشهود الذين قد يكونوا موجودين في مسرح الجريمة، وعليه قد يكون الفريق من شخصين أو أكثر.

**فريق الرسم والتصوير :**

ويضم شخصاً أو أكثر يقومون برسم الخرائط الكروكية لمسرح الجريمة وتحديد مواقع الأجهزة والملفات والأشخاص، والتقاط الصور الفوتوغرافية، والتصوير بالفيديو ـ مع مراعاة أن يتم تنبيه جميع العاملين في مسرح الجريمة عند استعمال الفيديو تحسباً لتسجيل أصوات المشاركين في التفتيش.

**فريق التفتيش العلمي :**

ويضم شخصاً واحداً أو أكثر، حسب الأحوال، ويتولى هذا الفريق عملية البحث والتدقيق على مسرح الجريمة وفقاً للنظم الفنية التي تُتبع في تفتيش الأماكن وتفتيش مسرح الجريمة، ويقوم هذا الفريق بالمرور على جميع الغرف والمخازن ويفحص المخازن، والمخابئ، وليس من الضروري أن يكون أعضاء هذا الفريق من خبراء الحاسب الآلي، ولكن يُفضّل أن يتم تنويرهم بالأشياء التي ينبغي البحث عنها.

**فريق التأمين والقبض :**

ويُعنىٰ هذا الفريق بالسيطرة أمنياً على مسرح الجريمة وضبط مخارجها ومنافذها وحركة الموجودين في المبنى والمباني المجاورة لمسرح الجريمة،وتنفيذ عملية القبض على المشتبه فيهم واحتجازهم وفق ما يأمر به المشرف، ويتكون هذا الفريق من رجال الأمن بالزي الرسمي.

**فريق ضبط وتحريز الأدلة :**

ويضم هذا الفريق اثنين أو أكثر من خبراء الحاسب الآلي يتولون ضبط وإدخال المعلومات المضبوطة في الحاسب الآلي وتصنيف الأدلة وتحريزها في الصناديق، ووضع العلامات الموضّحة عليها. ويقوم هذا الفريق بنقل أجهزة الحاسب الآلي المضبوطة بعد إجراءات الرسم والتصوير، ويجب أن يكون من بين أعضاء هذا الفريق شخصان على الأقل، أحدهما محقق في مجال الحاسب الآلي،والثاني خبير في الحاسب الآلي على التعامل مع الأدلة وطرق تقويمها.

**خبراء مسرح الجريمة العادية**

يتم اختيارهم حسب الحال، وقد يحتاج المحقق في بعض جرائم الحاسب الآلي كامل أعضاء الفريق أو بعضهم، مثل خبراء البصمات، المهندسين،خبراء المتفجرات[1] . . . . إلخ.

## الشهادة في مجال الجريمة المعلوماتية

**تعريف الشهادة وأهميتها :**

الشهادة هي الأقوال التي يدلى بها غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى

(1) راجع في ذلك : د. محمد الأمين البشري، سبقت الإشارة إليه، ص30 وما بعدها.

متهم أوبراءته منها [1]. وللشهادة في مجال الإجراءات أهمية بالغة لأن الجريمة ليست تطرفاً قانونياً ولكنها عمل غير مشروع يجتهد الجاني في التكتم عند ارتكابه ويحرص على إخفائه عن الناس.

ولهذا فإن العثور على شاهد يعتبر مكسباً كبيراً للعدالة ومن هنا جاءت قاعدة عدم رد الشهود.

**تعيين الشهود واستدعاؤهم :**

سماع الشهود كسائر اجراءات التحقيق من الأمور التقليدية للمحقق فله أن يسمع الشهود أو يستغني عنهم فإذا قرر سماعهم فهو الذي يحدد من يجب الاستماع إليه ومن يمكن الاستغناء عنه والأمر متروك إلى فطنة المحقق ومرتبط بظروف التحقيق، والأصل أن يطلب الخصوم سماع من يرون من الشهود غير أن للمحقق أن يجيبهم، بل له أن يسمع شهادة أي شاهد يتقدم من تلقاء نفسه. ومن المبادئ المستقرة أن الشاهد لا يُردّ ولو غلب على الظن أنه لن يتحرى الصدق في شهادته سواء كان ذلك راجعاً لانحطاطٍ في خلقه أو لوجود صلة مودة أو لعدواة بينه وبين المتهم تجعله يميل له أو ضده.

**المقصود بالشاهد في الجريمة المعلوماتية :**

يقصد بالشاهد في الجريمة المعلوماتية الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي والذي تكون لديه معلومات جوهرية أو هامة لازمة للولوج في نظام الجامعة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي وذلك تمييزاً له عن الشاهد التقليدي، ويشمل الشاهد المعلوماتي بهذا المفهوم عدة طوائف من أهمها :

---

(1) تعرِّف محكمة النقض المصرية الشهادة بأنها تقرير الشخص لما يكون قد رآه أو سمعه بنفسه أو أدركه على وجه العموم بحواسّه. (نقض 25 ـ 1 ـ 1976 أحكام النقض س27 ص94 رقم 20 و2/ 2/ 2978 س29ص139 رقم 25 و2/ 4/ 1979 س30 ص426 رقم 90).

**1 ـ القائم على تشغيل الحاسب الآلي**

وهو المسؤول عن تشغيل جهاز الحاسب الآلي والمعدات المتصلة به ويجب أن تكون لديه خبرة كبيرة في تشغيل الجهاز واستخدام لوحة المفاتيح في إدخال البيانات، كما يجب ان تكون لديه معلومات عن قواعد كتابة البرامج [1] .

**2 ـ المبرمجون :**

وهم الاشخاص المتخصصون في كتابة أوامر البرامج ويمكن تقسيمهم إلى فئتين :

الفئة الأولى : هم مخططوا برامج التطبيقات.

الفئة الثانية : هم مخططوا برامج النظم.

حيث يقوم مخططو برامج التطبيقات بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم ثم يقوم بتحويلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات. أما مخططو برامج النظم فيقوموا باختيار وتعديل وتصحيح برامج نظام الحاسب الداخلية أي أنه يقوم بالوظائف الخاصة بتجهيز الحاسب بالبرامج والأجزاء الداخلية التي تتحكم في وحدات الإدخال والاخراج ووسائط التخزين بالاضافة إلى إدخال أي تعديلات أو إضافات لهذه البرامج[2] .

**3 ـ المحللون :**

وهو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين، ودراسة هذه البيانات ثم تحليل النظام؛ أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقات الوظيفية من هذه الوحدات، كما يقوم بتتبع البيانات، داخل النظام عن

---

(1) انظر في ذلك :
د. محمد فهمي طلبة، الموسوعة الشاملة لمصطلحات الحاسب الآلي الإلكتروني، القاهرة، مطابع المكتب المصري الحديث، سنة 1991، ص23.

(2) انظر في ذلك : د. محمد فهمي طلبة، سبقت الإشارة إليه، ص37.

طريق ما يسمى بمخطط تدفق البيانات واستنتاج الأماكن التي يمكن مَيْكَنتها بوساطة الحاسب.

**4 ـ مهندسو الصيانة والاتصالات:**

وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب وبمكونات وشبكات الاتصال المتعلقة به.

**5 ـ مديرو النظم:**

وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية[1].

ويحصر قانون الدليل الخاص بولاية كاليفورنيا شهود الجريمة المعلوماتية في:

- محلل النُظم الذي صمّم وحدد برنامج الكمبيوتر الذي أنتج الدليل.
- المبرمج الذي قام بتحرير البرنامج واختباره.
- المشغّل الذي يقوم بتشغيل البرامج.
- طاقم عمليات البيانات الذي يعد البيانات بالصورة التي يستطيع الكمبيوتر قراءتها (شريط أو اسطوانة).
- أمناء مكتبة الأشرطة الذين يتحمّلون مسؤولية توفير الأشرطة أو الأسطوانات التي تشتمل على البيانات المصدرية الصحيحة.
- مهندس الصيانة الالكترونية الذي يقوم على صيانة الجهاز الأصلي والتأكد من عمله بصورة صحيحة.
- موظفو المدخلات والمخرجات والمسؤولين عن معالجة المدخلات والمخرجات يدوياً قبل وبعد أداء العمل.

---

(1) انظر في ذلك: د. محمد فهمي طلبه، سبقت الإشارة إليه، ص23.

- مبرمجو صيانة النظام والمسؤولون عن سرية عمله، ويصرح عمل الكمبيوتر المستخدم في تنفيذ برامجه.
- المستخدم النهائي الذي يمدّ بالمعلومات المدخلة ويصرح بتنفيذ برامج الكمبيوتر ويستخدم نواتجها[1].

**التزامات الشاهد المعلوماتي :**

يتعيّن على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعياً عن أدلة الجريمة بداخله. والسؤال الذي يطرح نفسه: هل يلتزم الشاهد بطبع الملفات والإفصاح عن كلمات المرور والشفرات ؟

هناك اتجاهان في هذا الصدد :

الاتجاه الأول :ويرى أنه ليس من واجب الشاهد وفقاً للالتزامات التقليدية للشهادة أن يقوم بطبع ملف البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة، ويميل إلى هذا الاتجاه الألماني حيث يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسب على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب[2].

الاتجاه الثاني : ويرى أنصار هذا الاتجاه أن من بين الالتزامات التي يتحمل بها الشاهد، القيام بملفات البيانات أو الإفصاح عن كلمات المرور او الشفرات الخاصة بالبرامج المختلفة[3] حيث يرى اتجاهٌ في الفقه الفرنسي أن

---

(1) بحث مقدم من مركز البحوث بشرطة دبي، عام 1998 للإمارات العربية المتحدة.

(2) انظر في ذلك

Mohrenschlager (Manfred): «computer crimes and other crimes against information technology in germany», R.I.D.P.1993P.351

(3) انظر في ذلك :

ERMAN (sahir) «les crimes infromatiques et d’autres crimes dans le domaine de la tecnologie infromatieque en torque,» R.I.D.P. 1993,P.624

القواعد العامة في مجال الإجراءات تحتفظ بسلطانها في مجال الإجراءات المعلوماتية ومن ثمّ يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهادتهم (المواد 62، 109، 138) من قانون الإجراءات الجزائية الفرنسي، ومن ثم يجب عليهم الإفصاح عن كلمات المرور السرية التي يعلمونها،ولكن ربط إعطاء المعلومات المطلوبة غير معاقب جنائياً إلا في مرحلة التحقيق والمحاكمة[1]. وفي هولندا يتيح مشرع قانون الحاسب الآلي لسلطات التحري والتحقيق إصدار الأمر للقائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراقه والولوج إلى داخله، كالإفصاح عن كلمات المرور السرية والشفرات الخاصة بتشغيل مختلف البرامج، وإذا وجدت بيانات مشفّرة أو مرمّزة داخل ذاكرة الحاسب وكانت مصلحة التحقيق تستلزم الحصول عليها، يتم تكليف القائم على تشغيل النظام المعلوماتي بحل رموز هذه البيانات[2].

وفي اليونان يمكن الحصول من القائم على تشغيل نظام الحاسب، على كلمة المرور السرية للولوج في النظام المعلوماتي، كما يمكن الحصول منه على بعض الإيضاحات الخاصة بنظامه الأمني، لكن ليس على الشاهد أي التزاماتٍ بالنسبة لطباعة ملفات بيانات مخزنة في ذاكرة الحاسب، وذلك لأنه يجب أن يشهد على معلومات حازها بالفعل وليس الكشف عن معلومات جديدة (المادة 323 فقرة 1 إجراءات جنائية يوناني)[3].

## الخبرة في مجال الجريمة المعلوماتية

هنا من المقرر أن يتم ندب خبير مع مراعاة مبررات ندبه وإجراءات هذا

---

(1) راجع في ذلك : DR.: Jacques franccillon op.cit.,p.309

(2) انظر في ذلك : Kasbersen op.cit., p. 496

(3) انظر في ذلك :
Vassilaki (Irini): computer crimes and other crimes against information technology in Greece, R.I.D.P.1993,P.371

الندب، حيث يرى المحقق في بعض الأحيان ضرورة الاستعانة بالخبير لإيضاح مسألة تستعصي ثقافة العامة عن فهمها، كتحديد سبب الوفاة أو ساعتها، أو رفع بصمة وجدت في مكان الجريمة، أو فحص سيارة لبيان ما فيها من خلل. وتكتسب الخبرة أهمية بالغة في مجال الجريمة المعلوماتية نظراً لأن الحاسبات وشبكات الاتصال بينها على أنواع ونماذج متعددة، كذلك فإن العلوم والتقنيات المتصلة بها تنتمي إلى تخصصات عملية وفنية دقيقة ومتنوعة، والتطورات في مجالها سريعة ومتلاحقة لدرجة قد يصعب معها على المتخصص تتبعها واستيعابها. ويمكن القول بصفة عامة، أنه لا يوجد حتى الآن خبير لديه معرفة متعمقة في سائر أنواع الحاسبات وبرامجها وشبكاتها، كذلك لا يوجد خبير قادر على التعامل مع سائر أنماط الجرائم التي تقع عليها أو ترتكب عن طريقها[1].

لذا ترك المشرّع للمحقق الحرية الكاملة في هذا الشأن ليمكنه من كشف الحقيقة بالسرعة اللازمة وبالطريقة التي يراها مناسبة[2]، وللمحقق في أي وقت ـ إلى أن ينتهي التحقيق ـ أن يندب من يأنس فيه الكفاية الفنية اللازمة للاستعانة بخبرته.

ونَدْبُ الخبير من سلطات المحقق، فليس في القانون ما يلزمه بالاستجابة للمتهم ولا لغيره من الخصوم إذا طلبوا ندب الخبير.

ويحدد المحقق للخبير مهمته والميعاد الذي سيقدم فيه تقريره، وعليه أن يحلّفه اليمين على أن يبدى رأيه بالذمة، وهذا الاجراء جوهري يترتب على

(1) راجع في ذلك :
PHILIP M. stanely computer crime invetigatoin and investigators computer & security North Holland 1986,pp.310-311
مشار إليه في : د. هشام محمد فريد رستم، مرجع سبقت الإشارة إليه.

(2) راجع في ذلك: Investigating computer crimes
Franklin clark den diliberto p. 147

إغفاله بطلان عمل الخبير[1]. والأصل أن يباشر الخبير عمله في حضور المحقق وتحت إشرافه، والاستثناء أن يتم في غيابه.

وللخصوم حق الحضور أثناء عمل الخبير ويجوز مع ذلك أن يباشر الخبير عمله في غياب الخصوم، وأن يمنعهم كذلك من الحضور إذا كان للمنع سبب. ويُعَدُّ الحصول على المستندات خلال عملية التفتيش أمراً سهلاً، حيث يمكن التعرف عليها بالرؤية، ولن يحتاج المحقق لأي مساعدة من قبل الخبراء، وهذه المستندات مثل: أدلّة عمل النظام، سجلات إدارة الكمبيوتر، وثائق البرامج والسجلات، صيغ مدخلات البيانات والبرامج. وكذلك صيغ مخرجات الكمبيوتر المطبوعة، ويتم التخطيط على هذه المستندات ويمكن تحديد ما إذا كانت كاملة أصلية، أو صوراً من خلال استجواب القائمين على حفظها.

وقد يكون التحفظ على المواد بوسائل الكمبيوتر الأخرى أمراً أكثر تعقيداً مثل: الأشرطة الممغنطة، الاسطوانات، البرامج، ويحتاج إلى معونة أحد الخبراء الموثوق فيهم، حتى يتمكن المحقق من الإلمام بمحتويات الأشرطة، أو الأسطوانات من دون إحداث أي تغيير فيها.

وبالطبع، فإن البحث عن المعلومات داخل جهاز الكمبيوتر ذاته يعد أمراً بالغ التعقيد ويحتاج إلى وجود خبير[2].

وأهم المسائل التي يستعان فيها بالخبرة في مجال الجرائم المعلوماتية هي:

---

(1) نقض مصري 26/ 12/ 1926 المحاماة س7ص789و 8/ 2/ 1927 ص8 ص1958 و1/ 3/ 1937 مجموعة القواعد القانونية جـ4، ص52، رقم 43.

(2) راجع في ذلك:
بحث مقدم من مركز البحوث والدراسات بشرطة دبي ـ الإمارات العربية المتحدة بعنوان: جرائم الكمبيوتر سنة 1998 ص2.

**أولاً : ما يتعلق بالوصف**

أ - تركيب الحاسبات وصناعتها وطرازها، ونوع نظام التشغيل وأهم الأنظمة الفرعية التي يستخدمها، بالإضافة إلى الأجهزة الطرفية الملحقة بها، وكلمات المرور أو السر ونظام التشفير. . .إلخ.

ب - بيئة الحاسب أو الشبكة، من حيث تنظيم،ومدى تركيز أو توزيع عمل المعالجة الآلية، ونمط وسائط الاتصالات، وتردد موجات البث وأمكنة اختزانها.

ج - الموضع المحتمل لأدلة الإثبات والشكل أو الهيئة التي تكون عليها.

د - أثر التحقيق من الوجهة الاقتصادية والمالية على المشاركين في استخدام النظام.

**ثانياً : ما يتعلق بالبيان**

أ - كيف يمكن، عند الاقتضاء، عزل النظام المعلوماتي دون إتلاف الأدلة أو تدميرها أو إلحاق ضرر بالأجهزة.

ب - كيف يمكن، عند الاقتضاء، نقل أدلة الإثبات إلى أوعية ملائمة من غير أن يلحقها تلف.

ج - كيفية تجسيد الأدلة في صورة مادية بنقلها، إذا أمكن، إلى أوعية ورقية يتاح للقاضي مطالعتها وفهمها، مع إثبات أن المسطور على الورق مطابق للمسجَّل على الحاسب أو النظام أو الشبكة أو الدعامة الممغنطة[1].

## الضبط في مجال الجريمة المعلوماتية

**معنى الضبط وطبيعته :**

يقصد بالضبط في قانون الاجراءات الجنائية، وضع اليد على شيء يتصل

(1) انظر في ذلك : د. هشام محمد فريد رستم، سبقت الإشارة إليه، ص41

بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها، وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو التحقيق.

وتحدد طبيعته بحسب الطريقة التي يتم بها وضع اليد على الشيء المضبوط. فإذا كان الشيء وقت ضبطه في حيازة شخص واقتضى الأمر تجريده من حيازته، كان الضبط نظيرَ إجراءِ تحقيق، أما إذا كان الاستيلاء عليها دون الاعتداء على حيازة قائمة، فإنه يكون نظيرَ إجراء استدلال.

**محل الضبط :**

الضبط بطبيعته، وبحسب تنظيمه القانوني وغايته، لا يَرِدُ إلا على الأشياء، أما الأشخاص فلا يصلحون محلاً للضبط بالمعنى الدقيق، وإذا كان قانون الإجراءات يتحدث في بعض النصوص عن ضبط الأشخاص وإحضارهم فإنه يعني القبض عليهم وإحضارهم. والقبض نظام قانوني يختلف تماماً عن ضبط الأشياء.

ولا يفرق القانون في مجال الضبط بين المنقول والعقار، فكلاهما يمكن ضبطه، كذلك فإنه يستوي أن يكون الشيء المضبوط مملوكاً للمتهم أو لغيره، والقاعدة لا يَرِدُ إلا شيءٌ مادي أما الأشياء المعنوية فلا تصلح بطبيعتها محلاً للضبط، والشرط اللازم لصحة الضبط أن يكون الشيء مفيداً في كشف الحقيقة، فكل ما يحقق هذه الغاية يصحُّ ضبطه.

والأدلة المادية التي يجوز ضبطها في الجريمة المعلوماتية والتي لها قيمة خاصة في إثبات جرائم ونسبتها إلى المتهم هي :

**1 ـ الورق :**

كثير من الجرائم الواقعة على المال، أو على جسم الإنسان، تترك خلفها قدراً كبيراً من الأوراق والمستندات الرسمية منها والخاصة،إلا أن وجود أجهزة الحاسب يجعل كثيراً من المعلومات يتم حفظها في الحاسب الآلي، ما قلّل من حجم الأوراق والملفات. ومع ذلك نجد أن الكثيرين يقومون بطباعة المعلومات لأغراض المراجعة،أو التأكد من الشكل العام للمستند أو الرسالة أو الرسومات

موضوع الجريمة،وأجهزة الحاسب الآلي والطابعات المتطورة ذات السرعة الفائقة تطبع قدراً كبيراً من الأوراق في وقت قصير. وعليه، يعتبر الورق من الأدلة التي ينبغي الاهتمام بها في البحث وتفتيش مسرح الجريمة. والورق أربعة أنواع:

أ - أوراق تحضيرية يتم إعدادها بخط اليد كمسوّدة أو تصور للعملية التي يتم برمجتها.

ب - أوراق تالفة تتم طباعتها للتأكد، ومن ثم القاؤها في سلة المهملات.

ج - أوراق أصلية تتم طباعتها والاحتفاظ بها كمرجع، أو لأغراض تنفيذ الجريمة.

د - أوراق أساسية وقانونية محفوظة في الملفات العادية أو دفاتر الحسابات، وتكون لها علاقة بالجريمة، بخاصةٍ عند تقليدها أو تزوير بياناتها لتنفيذ جريمة الحاسب الآلي.

**2 - جهاز الحاسب الآلي وملحقاته :**

وجود جهاز حاسب آلي مهمٌّ للقول بأن الجريمة جريمة حاسب آلي، وأنها مرتبطة بالمكان أو الشخص الحائز على الجهاز. ولأجهزة الحاسب الآلي أشكال وأحجام وألوان مختلفة، وخبير الحاسب الآلي يستطيع ان يتعرف على الحاسب الآلي ومواصفاته بسرعة فائقة،كما يستطيع تمييزه عن الأجهزة الإلكترونية الأخرى وتحديد أسلوب التعامل معه في حالة الضبط والتحريز.

ومن السهل التعرف على جهاز الحاسب الآلي الشخصي الذي أصبح مألوفاً اليوم، فهو يتكون من وحدة المعالجة المركزية، لوحة المفاتيح والشاشة، ومع التطورات السريعة التي يمر بها الحاسب الآلي نجد إضافات جديدة مثل المودم والماوس والسماعات والسيرفر. وإذا كنا بصدد الحديث عن الأجهزة الكبيرة فإننا نجد أن أشكالها تتغير باستمرار خصوصاً من حيث الحجم والهيكل.

ومن الضروري إطلاع العاملين في مجال التحقيق على مختلف أشكال أجهزة الحاسب الآلي فور ظهورها.

**3 ـ أقراص الليزر**

مع أي جهاز شخصي عادي تجد قدراً كبيراً من أقراص الليزر، علاوة على أن مراكز الحاسب الآلي في الشركات والبنوك تجد فيها الآلاف من الأقراص، وقد تكون على غلاف القرص بيانات توضح محتويات القرص، إلا أن ذلك لا يعتد به في التحقيق الذي يتطلب بيانات دقيقة عن محتويات كل قرص وبمعرفة خبير يقدم الدليل أمام المحكمة، وقد تجد في مكان ما أقراص الليزر ولا نجد معها أجهزة حاسب آلي، ومع ذلك يعد جزءاً من جريمة حاسبٍ آلي متى كانت محتوياتها عنصراً من عناصر الجريمة.

**4 ـ الشرائط الممغنطة**

تستعمل الشرائط الممغنطة عادة للحفظ الاحتياطي، وقد تكون في مكان بعيد آمن، كما يقوم البعض بإيداعها في خزائن البنوك التجارية أو مراكز التوثيق الحكومية الآمنة.

**5 ـ لوحة الدوائر**

**6 ـ المودم**

المودم هي الوسيلة التي تمكّن أجهزة الحاسب الآلي من الاتصال، بعضُها مع بعض، عبر خطوط الهاتف. وقد تطورت المودم إلى أجهزة إرسال الفاكس والرد على المكالمات الهاتفية وتبادل البيانات وتعديلها. وللمودم أشكال وهياكل تتطور مع تطور تقنية صناعة الحاسب الآلي.

**7 ـ الطابعات**

والطابعات أنواع، منها العادية ومنها طابعات ليزرية، الملوَّنة منها وغير الملونة.

8 ـ PEMCIA CARDS :

وتستعمل بطاقات في أجهزة الحاسب الآلي الصغيرة النوت، بوك واللاب توب، وهي في شكل البطاقات الائتمانية.

**9 ـ البرامج اللينة والمراشد :**

المراشد المصاحبة للحاسب الآلي مفيدة في التعرف على الجهاز والبرامج المستعملة فيها.

10 ـ البطاقات الممغنطة وبطاقات الائتمان القديمة والمواد البلاستيكية المستعملة في إعداد تلك البطاقات، تعتبر قرائن للإثبات في جرائم الحاسب الآلي.

كل ذلك يُعدّ أثراً أو جزءاً من جسم الجريمة ينبغي البحث عنها وفحصها والاستفادة منها في التحقيق، علماً بأن التعامل مع مثل هذه الآثار يحتاج إلى خبرة فنية في مجال الحاسب الآلي ومعرفة بالقانون وقواعد البيئة [1]

## المبحث الثانـي:
## صعوبات جمع الأدلة في مجال جرائم سرقة المعلوماتية والإنترنت

إن أهم ما يميز جرائم نظم المعلومات صعوبة اكتشافها واثباتها وهى صعوبة يعترف بها جميع الباحثين في هذا المجال[2]. علاوة على ما تتميز به اجراءات جمع الأدلة في هذا المجال من ذاتية خاصة.

---

(1) راجع في ذلك : د. محمد الأمين البشري، سبقت الإشارة إليه ص33.

(2) انظر في ذلك : د. محمد زكي ـ الإثبات في المواد الجنائية، ص16، د.محمد محيي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، ص398 ـ 399 د. هدى حامد قشقوش، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 25 ـ 28 أكتوبر/ت1 1993، منشورات دار النهضة العربية 1993، ص450 و476 و576. د. زكي أمين حسونة، جرائم =

وتنقسم المعوقات في هذا الصدد إلى عدة أنواع نفصّلها فيما يلى:

## معوقات خاصة بطبيعة الجريمة وأدلتها

### أولا: المعوقات الخاصة بطبيعة الجريمة (جريمة غير مرئية):

تتسم الجرائم التي تقع على الحاسبات وشبكات المعلومات بأنها غير مرئية في العديد من حالاتها[1]. حيث لا يلاحظها المجنيُّ عليه غالباً أو يعلم حتى بوقوعها.

وإخفاء السلوك المكون لها وطمس أو تغطية نتائجها عن طريق التلاعب غير المرئى في النبضات أو الذبذبات الإلكترونية التي تسجل البيانات عن طريقها ليس مستحيلاً في الكثير من أحوالها، بحكم توافر المعرفة والخبرة الفنية في مجال الحاسبات لدى مرتكبها.[2]. اختلاس المال عن طريق التلاعب في برامج الحاسب ومحتوياته، وغالباً ما يتم في مخرجات الحاسب تغطية وستره.

---

= الكمبيوتر والجرائم الأخرى في مجال التكتيك المعلوماتي ـ بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي القاهرة، 25 ـ 28 أكتوبر/ ت1 1993، العقيد علاء الدين محمد شحاته ـ رؤية أمنية للجرائم الناشئة عن استخدام الحاسب الآلي ـ بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي ـ القاهرة 25 ـ 28 أكتوبر/ ت1 1993.

(1) انظر في ذلك: إذ تقع هذه النوعية من الجرائم في بيئة لا تعتمد التعاملات فيها أصلاً على الوثائق والمستندات المكتوبة بل على نبضات اليكترونية غير مرئية لا يمكن قراءتها إلا بوساطة الحاسب الآلي والبيانات التي يمكن استخدامها كأدلة ضد الفاعل يمكن في أقل من الثانية العبث بها أو محوها بالكامل، لذا فإن للمصادفة وسوء الحظ دوراً في اكتشافها يفوق دور أساليب التدقيق والرقابة ومعظم مرتكبيها الذين تم ضبطهم وفقاً لما لاحظه أحد الخبراء، إما أنهم قد تصرفوا بغباء أو أنهم لم يستخدموا الأنظمة المعلوماتية بمهارة: انظر:

John Eaton and Jermy smithers, this is it. Amangagrs Guide to information technology, London, Philip Allan, 1982 p.263

مشار إليه د. هشام محمد فريد رستم، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت في الفترة من 1 ـ 3 مايو/ أيار 2000 بجامعة الإمارات العربية المتحدة بعنوان الجرائم المعلوماتية.

(2) انظر في ذلك:

Jay, J. Becker the Trial of computer crime (1980), 2 computer Law, Journal 441

الدكتور هشام محمد فريد رستم، سبقت الإشارة إليه.

والتجسس على ملف البيانات كان خطأً مصدره البرامج أو الأجهزة أو نظام التشغيل أو التصميم الكلّي للنظام المعلوماتي.

ونتيجة لهذه الصعوبة أصبح لإمكانية أخفاء الجريمة المعلوماتية عن طريق التلاعب في البيانات مصطلح، يستخدم في أبحاث علم الإجرام الأمريكية وهو (الطبيعة غير الأولية لمخرجات الحاسب المطبوعة)[1]، Second-hand Nature computer printouts.

### ثانياً : معوقات خاصة بأدلة الجريمة:

#### (أ) انعدام الدليل المرئي:

يلاحظ أن ما ينتج عن نظم المعلومات من أدلة عن الجرائم التي تقع عليها أو عَبْرها، ما هى إلا بيانات غير مرئية لا تفصح عن شخصية معينة وهذه البيانات مسجلة إلكترونياً بكثافة بالغة وبصورة مُرمّزة. غالباً على دعائم أو وسائط للتخزين ضوئية كانت أو ممغنطة، لا يمكن للإنسان قراءتها وإن كانت قابلة للقراءة من قبل الآلة نفسها، ولا يترك التعديل أو التلاعب فيها أي أثر، مما يقطع أيّ صلة بين المجرم وجريمته ويعوق، أو يحول، دون كشف شخصيته[2]. وإنّ كشف وتجميع أدلة بهذا الشكل لإثبات وقوع الجريمة والتعرف على مرتكبيها هو أحد أبرز المشاكل التي يمكن أن تواجه جهات التحري والملاحقة.

وتبدو هذه المشكلة بشكل عام في سائر مجالات التخزين والمعالجة الآلية للبيانات، حيث تنتفي غالباً قدرة ممثلى الجهات المختصة على أن يتولوا بطريقة مباشرة فحص واختبار البيانات المشتبه فيها، وتزداد جسامة هذه المشكلة

---

(1) Les dificultes techniques sont liees aux methoded de cryptologie employees sur le reseua.
La criminamite informatique sur linternet, p. 58

(2) انظر في ذلك : Ulrich, sieber, ibid, p. 140

بوجه خاص في حالة التلاعب في برامج الحاسب نظراً لتطلب الفحص الكامل للبرنامج واكتشاف التعليمات غير المشروعة المخفية داخله، قدراً كبيراً من الوقت والعمل، وغالباً ما لا يكون له من حيث التكلفة الاقتصادية مبرر(1).

**(ب) سهولة محو الدليل أو تدميره في فترة زمنية يسيرة:**

من الصعوبات التي يمكن أن تعترض عملية الإثبات في مجال جرائم نُظُم المعلومات، سهولة محو الجاني أو تدميره أدلّة الإدانة في فترة زمنية وجيزة، فضلاً عن سهولة تنصله من هذا العمل بإرجاعه إلى خطأ في نظام الحاسب أو الشبكة أو في الأجهزة. ومن الأمثلة الواقعية قيام أحد مهربى الأسلحة بإدخال تعديلات على الأوامر العادية لنظام تشغيل حاسب صغير يستخدمه في تخزين عناوين عملائه والمتعاملين، معه بحيث يترتب على إدخال أمرٍ إلى الحاسب من خلال لوحة مفاتيحه بالنسخ أو الطبع أو تدمير البيانات كلها.

ومع أن تعديل برمجة نظام تشغيل الحاسب كان قد أجري خصيصاً بواسطة الفاعل للحيلولة دون نجاح أجهزة الملاحقة في الإجراءات المتوقعة

---

(1) راجع في ذلك : وتدليلا على تأثير غياب الدليل المرئي في إعاقة إجراءات الضبط وملاحقة مرتكبي الجرائم التي تقع في مجال تكنولوجيا المعلومات، يشير الأستاذ sieber إلى حالة واقعية شهدتها ألمانيا الاتحادية سابقاً عام 1971 تلخص وقائعها في اكتشاف شركة طلبياتها بريدية mail order firm سرقة أشرطة ممغنطة تخصها تحوي 300000 عنوانٍ لعملاتها وتمكنها من استصدار أمر من المحكمة، معروف باسم وقف الأعمال injuction، باستعادة كل العناوين من شركة منافسة كانت قد حصلت على هذه العناوين من مرتكبي السرقة، وتنفيذاً لهذا الأمر سمحت الشركة المنافسة لمساعدة مأمور التنفيذ بدخول مقرها ومركز الحاسب الخاص بها، حيث وجد [هذا المأمور] نفسه أمام كم هائل من الأشرطة والأقراص الممغنطة التي لا يدري عنها شيئاً أو يعرف محتوياتها أو لديه القدرة على فحصها ومعرفة مضمونها، مما اضطره إلى مغادرة مركز حاسب الشركة المنافسة خالي الوفاض. ومع أن الشركة المنافسة قامت من تلقاء نفسها بعد ذلك بعدة أيام بتسليم بيانات العناوين إلى الشركة المجني عليها إلا أنه من الوارد بالتأكيد ـ أن تكون الأشرطة المعنية قد تم استنساخها قبل تسليمها، وهو ما يكون قد أفقد أمر المحكمة جدواه.
راجع Ulrich siber, ibid,p. 140 .

للبحث عن الأدلة وضبطها إلا أنه لم يفلح في تحقيق هذا الهدف نتيجة لتوقع المتخصصين لمعالجة البيانات في الجهاز المركزي لمكافحة الغش المعلوماتي بالنمسا بأن شيئاً ما في نظام تشغيل حاسب الفاعل قد جرى تغييره وقيامهم بناءً على ذلك باستنساخ الأقراص الممغنطة المضبوطة، عن طريق أنظمة حاسباتهم[1].

وفى حالة أخرى شهدتها ألمانيا الاتحادية سابقاً، أدخل الجناة في نظام الحاسب تعليمات أمنية لحماية البيانات المخزنة داخله من المحاولات الرامية إلى الوصول إليها ومن شأنها محو هذه البيانات بالكامل بوساطة مجال كهربائي وذلك إذا ما تم اختراقه من قبل شخص غير مرخص له[2].

### (جـ) صعوبة الوصول إلى الدليل:

تحاط البيانات المخزنة إلكترونياً أو المنقولة عبر شبكات الاتصال بجدار من الحماية الفنية لإعاقة محاولة الوصول غير المشروعة إليها للاطلاع عليها أو استنساخها[3]. . كذلك يمكن للمجرم المعلوماتي أن يزيد من صعوبة عملية التفتيش التي قد تباشر للحصول على الأدلة التي تدينه عن طريق مجموعة من

---

(1) راجع في ذلك : د. هشام محمد فريد رستم، سبقت الإشارة إليه، ص35 ـ 36.

(2) راجع في ذلك : Ulrich sieber, ibid, p. 141

(3) تواجه عملية جمع الأدلة الإلكترونية واستعمالها بعض التحديات الرئيسية major challenges ومنها :

- صعوبة الوصول إلى الملفات المحذوفة أو المخبأة أو المحمية بموجب كلمات مرور داخل النظم الضخمة المرتبطة من خلال الشبكات.
- صعوبة استعادة البيانات من بعض الوسائل أو الوسائط القديمة.
- صعوبة العثور على الملفات أو السجلات المحورية من بين المجالات الشاسعة للبيانات (مثال : سجلات البريد الإلكتروني)
- صعوبة تحليل صحة الملفات ـ ومعرفة ما إذا كان قد تم تعديلها او محوها :

راجع في ذلك : Linda volonino ph. D.ibid., p.14

التدابير الأمنية كاستخدام كلمة السر للوصول إليها أو دسّ تعليمات خفية بينها أو ترميزها لإعاقة أو منع الاطلاع عليها أو ضبطها. لذا فإن استخدام تقنيات التشفير لهذا الغرض يعد إحدى العقبات الكبرى التي تعوق رقابة البيانات المخزنة أو المنقولة عبر حدود الدولة، والتي تقلل من قدرة مختلف جهات التحرى والتحقيق والملاحقة على الاطلاع عليها الأمر الذى يجعل حماية حرمة البيانات الشخصية المخزنة في مراكز الحاسبات والشبكات، أو المتعلقة بالأسرار التجارية العادية والإلكترونية أو بتدابير الأمن والدفاع أمراً بالغ الصعوبة[1].

وتصطدم عقبة الوصول إلى الدليل المعلوماتي بمشكلة إجرائية تتعلق بمدى سريان القيود الخاصة بضبط الأوراق على ضبط محتوى نظام المعالجة الآلية للبيانات والمحميّ فنياً في مواجهة الاطلاع غير المسموح به، حيث يحظر قانون الإجراءات الجنائية المصرية والإماراتي بمقتضى المادتين 52، 58 على التوالى [2]، اطلاع مأمور الضبط القضائي على الأوراق المختومة أو المغلقة[3]. الموجودة في منزل المتهم أثناء تفتيشه[4]. وعلة ذلك الحفاظ على الآثار التي تتضمنها الأوراق. وهنا يثور تساؤل عما إذا كان حكم هاتين المادتين واجب

---

(1) انظر في ذلك: يشير الأستاذ sieber بأن مشاكل عديدة لا يستهان بها قد نجمت من استخدام الجناة في بعض الجرائم المعلوماتية التي وقعت بألمانيا الاتحادية سابقاً لتقنيات التشفير أو الترميز لإعاقة اكتشاف أو الوصول إلى أدلة تدينهم، وبوجه خاص في مجال وسائل التخزين التي يصعب ضبطها.

راجع في ذلك: Ulrich Sieber Ibid, p. 141

(2) تنص المادة الأولى منهما على أنه «إذا وجدت في منزل المتهم أوراق مختومة أو مغلقة بأية طريقة فلا تجوز لمأمور الضبط القضائي أن يفضها، وبالصياغة ذاتها تقريباً يسري نص المادة 58 أ.ج. إماراتي.

(3) فإذا كانت ظاهرا أن التغليف لا ينطوي وإنما يحوي جسما صلبا، فإنه يجوز لمأمور الضبط القضائي فض الغلاف لفحص محتوياته نقض مصري 24 يونية 1958، مجموعة أحكام النقض س9 رقم 180 ص716.

(4) قضى في مصر بعدم دستورية المادة 47 من قانون الإجراءات الجنائية المصري في 2 يونيه 1984 ومن ثم لم يعد هناك مجال لتطبيق نص المادة 52 من هذا القانون في حالة التلبس بالجريمة.

الإتباع بالنسبة لإطلاع مأمور الضبط القضائي على محتوى نظام المعالجة الآلية للبيانات من عدمه وذلك في حالة ما إذا كان محاطاً بجدار من الحماية الفنية تعوق الاطلاع عليه. ونبادر بالإجابة على هذا التساؤل استناداً إلى سببين :

الأول : أن السبب الذي من أجله تم تقرير هذا الحكم بالنسبة للأوراق المختومة أو المغلقة يتوافر أيضاً بالنسبة لمحتوى نظام المعالجة الآلية للبيانات المحميّ فنياً ضد الإطلاع غير المسموح به.

فحظر المشرّع اطلاع مأمور الضبط القضائى على هذه الأوراق إنما هو لِمَظنَّةِ أن الغلق أو التغليف يضفى عليها مزيداً من السرية ويفصح عن رغبة صاحبها في عدم اطلاع الغير على مضمونها بدون إذنه وهو ما يتحقق في البيانات المخزنة أو المنقولة عبر نظام أو شبكة حاسب إذا كانت محمية فنياً ضد الاطلاع غير المسموح به. فمحتوى النظام لا يكون بذلك مكشوفاً بل محجوباً عن الغير حيث لا يتاح الوصول والاطلاع عليه بغير معرفة طريق ومفاتيح وكود التشغيل[1].

الثاني : أن المادة 52 إجراءات مصري (58 إجراءات إماراتي) تضع قاعدة عامة لضمان الأسرار التي تحتويها سائر وسائط وأوعية حفظ وتخزين ونقل المعلومات، سواءٌ ما كان منها تقليدياً كالأوراق، أو مستحدثاً كالأقراص المرنة والأشرطة الممغنطة والذكرات الداخلية للحاسبات وشبكات المعلومات المحلية والإقليمية والعالمية.

والجدير بالإشارة إليه أن كلاً من التشريعين الإجرائيين، المصرى والإماراتي لا ينفردان بهذه النتيجة بل يشاركهما فيها العديد من القوانين، ومنها

(1) راجع في ذلك :
د. هشام محمد فريد رستم، سبقت الإشارة إليه ص34.

على سبيل المثال قانون الاجراءات الجنائية الألماني، فطبقاً للمادة 110 منه تقتصر سلطة الاطلاع على مخرجات الحاسب وغيرها من دعائم البيانات على المدعي العام وحده، ولا يكون لضباط الشرطة حق الاطلاع على البيانات عن طريق تشغيل البرامج أو الاطلاع على ملفات البيانات المخزنة داخل الحاسب بغير إذن من له حق التصرف فيها، وما لهم قانوناً هو فحص دعائم البيانات عن طريق النظر فحسب دون استخدام مساعدات فنية[1]

**(د) افتقاد الآثار المؤدية إلى الدليل:**

يحدث في بعض الأحيان إدخال البيانات مباشرة في نظام الحاسب دون تطلب وجود وثائق معاونة (وثائق خاصة بالإدخال) كما هو الحال في بعض نظم العمليات المباشرة التي تقوم على استبدال الإذن الكتابي لإدخال البيانات بإجراءات أخرى تعتمد على ضوابط للإذن متضمنة في برنامج الحاسب (مثل المصادقة على الحد الأقصى للائتمان. وفي مجال العمليات المالية قد يباشر الحاسب بعض العمليات المحاسبية دونما حاجة إلى إدخالٍ كما هو الحال لاحتساب الفائدة على الإيداعات البنكية وقيدها آليا بأرصدة حسابات العملاء على أساس الشروط المتفق عليها مسبقاً والموجودة في برنامج الحاسب.

ويكون من السهل في كل من هذين النوعين من العمليات ارتكاب بعض أنواع من الجرائم، كاختلاس المال والتزوير بإدخال بيانات غير معتمدة في نظام الحاسب أو تعديل برامجه أو البيانات المخزنة داخله دون أن يترتب على ذلك أي أثر يشير ألى حدوث هذا الإدخال أو التعديل. لذا يتعين على المحقق إزاء صعوبة الوصول إلى مرتكبي الجرائم في كلا هذين النوعين من العمليات وعدم ترك التغيرات في البرامج أو البيانات آثار كتلك التي يخلّفها التزوير المادي في

(1) انظر في ذلك :
Manfred Mothren schlager, computer crimes and other crimes against information technology in Bermany, rev, inter, D.P. leret 2e trimesters 1993,p.351

المحررات التقليدية[1] أن يسعى لتحديد دائرة الأشخاص القائمين أو المتصلين في عمليات إدخال ومعالجة البيانات وغيرها من عمليات التسجيل[2]، مع الاستفادة من ضوابط الرقابة التي تباشر في النظام المعلوماتي على الإدخال والمعالجة إضافة إلى تتبع الأموال المختلفة، إن وجدت، باعتبارها محصلة الجريمة التي يستولي عليها المجرم في نهاية الأمر[3].

## المعوقات الخاصة بالعامل البشرى

ويتعدد هذا النوع من المعوقات على النحو التالى:

**1 ـ مكان ارتكاب الجريمة:**

يتمّ ارتكاب جريمة الحاسب الآلي عادةً عن بُعْد، حيث لا يكون الفاعل على مسرح الجريمة، ومن ثَمّ تتباعد المسافات بين الفعل (من خلال حاسب الفاعل) و النتيجة (المعطيات محل الاعتداء) وهذه المسافات لا تقف عند حدود الدولة بل قد تمتد إلى النطاق الإقليمى لدول أخرى، ما يضاعف صعوبة كشفها أو ملاحقتها[4].

فقد أعلنت السلطات البريطانية أن أكثر من عشرة آلاف أَسطوانة تعليمية عن الإيدز قد أدخلت إلى المستشفيات في كل من بريطانيا والسويد والدنمارك والنرويج.

---

(1) راجع في ذلك:
Jack Bologena corporate faraud: the Basice of prevention and detection, Butterworth publishers 1984,p.75

(2) راجع في ذلك: J.Tappolet, La fracuc infromatieque, rev, int, crim poltech 1988,p.351

(3) راجع في ذلك: د. هشام محمد فريد رستم، سابق الإشارة إليه ص31.

(4) راجع في ذلك: د. أسامة محمد محي الدين عوض، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 25 ـ 28 أكتوبر/ت1 1993.

وقد اكتشفت أجهزة البيانات أنها مصابة بفبروس «نورجان» وهو فيروس يؤدي إلى تخريب أجهزة الكمبيوتر الشخصى وإتلاف البرامج التي تعمل عليه. وفى غضون ذلك، بدأت شرطة سكوتلانديارد تحقيقات واسعة النطاق في هذه القضية باعتبارها جريمة تخريب، وقد أثبتت التحقيقات مايلى:

(أ) أن هذه الأسطوانة وصلت إلى الأشخاص بالبريد من مصادر مختلفة بهدف تخريب البرامج المرسلة إليهم، وأن أسماء الذين وجهت لهم الأسطوانات يبلغ عددهم نحو سبعة آلاف شخص، قد تم بيعها إلى شركة تدعى «كيتيما» وهى مؤسسة تخص رجل أعمال كينى «يدعى كيتيما»، وقد اتضح أن قائمة الأسماء التي أحضرت معه خلال زيارته لبريطانيا في الفترة من 31 أكتوبر/ ت1 حتى 30 نوفمبر/ ت2 1989 ولكنه لم يستدل منها له على عنوان.

(ب) أنّ عدداً من هذه الأسطوانات ظهرت في كاليفورنيا، وفي بلجيكا وزيمبابوي.

(ج) الرسائل أرسلت مع رسائل معنونة بـ «معلومات عن الإيدز» لكن تبين أنها تحتوى على فيروس نورجان الذى يهاجم أجهزة الحاسب الشخصي من نوع I. B. M والمتوافقة معه.

(د) تسأل الرسالة المرفقة مع الأسطوانة عن رسوم ملكية للبرنامج بمقدار 189 دولاراً أو 378 دولاراً حسب الطلب وإرسال الرد إلى عنوان في بنما، ولكن تبين أن معظم الرسائل أرسلت من لندن وبالتحري تبين عدم وجود شركة بهذا الاسم ولا يوجد لها صندوق بريد في بنما. بينما تبين أن مرسل الرسالة استخدم الاسم الأول من إحدى شركات البرامج الأمريكية العاملة في بنما والتى أكدت عدم مسؤوليتها عما حدث.

(و) تحذر الرسالة من أنه في حالة عدم دفع الرسوم سيستخدم المرسل برنامجاً

لتخريب المعلومات ووقف جهاز الكمبيوتر بشكل تلقائي. ولكن ما أثار الانتباه إلى هذه القضية حدث خلال تحميل الاسطوانة، وفقاً لما قاله «جرسيرست» خبير الفيروسات ومستشار التطبيقات البريطانى [1].

**2 ـ نقص خبرة الشرطة وجهات الادعاء والقضاء**

يتطلب كشف جرائم الكمبيوتر والوصول إلى مرتكبيها وملاحقتهم قضائيا استراتيجيات خاصة تتعلق بإكسابهم مهارات خاصة وعلى نحو يساعدهم على مواجهة تقنيات الحاسب الآلي المتطورة وتقنيات التلاعب به، حيث تنعقد وتتنوع التقنيات المرتبة بوسائل ارتكابها[2].

لذا يجب استخدام أساليب وتقنيات تحقيق جديدة ومبتكرة لتحديد نوعية الجريمة المرتكبة وشخصية مرتكبها وكيفية ارتكابها مع الاستعانة بوسائل جديدة أيضاً لضبط الجاني والحصول على أدلة إدانته.

إذ من المتصور أن يجد مأمورو الضبط القضائي أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذه النوعية من الجرائم[3]. ومما يزيد من صعوبة هذا الأمر افتقار أنظمة الحاسبات وشبكات المعلومات في البدايات الأولى لاستخدامها لأساليب الرقابة وضوابط التدقيق والمراجعة على العمليات والتطبيقات وعدم تزويدها بوسائل فنية لاكتشاف وتتبع

(1) راجع في ذلك : د. أسامة محمد محيي الدين عوض، سبقت الإشارة إليه، ص430 ـ 431.

(2) انظر في ذلك :

Donn, B., Parkar, vulnerabilities of EFT systm to intentionally causes losses in computers and Banking electronic funds transfer system and public poliecy edited by Kent w.colton and Keneth L. Kraemer, plenum press 1980,p. 97

(3) جاء بتوصية المجلس الأوروبي رقم (95) 13 في 11 سبتمبر/ أيلول 1995 في شأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات ضرورة تشكيل وحدات خاصة لمكافحة جرائم الحاسب وإعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات.

مسار العمليات[1]، فضلاً عن ما تصادفه هذه الجهات من صعوبات في التحري عن جرائم الحاسب عابرة الحدود لا سيما بعد انتشار استخدام شبكة المعلومات العالمية.

وكثيراً ما تفشل أجهزة الشرطة في تقدير أهمية الجريمة المعلوماتية نظراً لنقص الخبرة والتدريب[2]. وللسبب ذاته أيضاً كثيراً ما تفشل جهات التحقيق في جمع أدلة جرائم الحاسب الآلي، مثل مخرجات الحاسب وقوائم التشغيل، بل إن المحقق كما هو الحال أحياناً في بعض الجرائم الأخرى، قد يدمّر الدليل بمحوه الأسطوانة الصلبة بسبب خطأ منه أو إهمال أو بالتعامل مع الأقراص المرنة، أو بالتعامل المتسرع أو الخاطئ مع الأدلة[3].

تكمن المشكلة فيما يقوم به رجال الشرطة حين يستخدم الكمبيوتر كأداة

---

(1) راجع في ذلك:
Bernard P. zajac Jr. police responses to computer crime in the united states the computer law and security report July - auyg 1985,pp.16-17

(2) لقد علمت أن شاباً طلب نسخة أسطوانة كمبيوتر وقام بتصوير البطاقة الملصقة عليها ثم قام بوضع الأسطوانة على السطح الزجاجي لآلة التصوير إلا أن الاستاتيكية التي نشأت عندما عملت الآلة أدت إلى مسح وإمالة جميع المعلومات المسجلة على الأسطوانة. وهناك حالة أخرى، حيث قام رجال الشرطة بوضع حقيبة كاملة تحتوي على أسطوانات الكمبيوتر المصادرة وذلك في صندوق السيارة بالقرب من جهاز الإرسال والاستقبال اللاسلكي فكانت النتيجة أن الإشارات الكهربائية القوية تسببت في تدميرها جميعاً.
انظر في ذلك: Burici sterling ibid, p. 208
وصرح مكتب التحقيقات الفيدرالي بأن خبارته لم يتمكنوا من تحديد ما إذا كان الحدث قد وقع بسبب عطل فني أو هجوم ماكر وقد حجب الموقع الخاص بشركة السمسمرة الوطنية والذي يرتاده 200 ألف عميل لمدة تفوق الساعة ـ حاول خلالها مهندسوا الشركة الدفاع عن النظام ضد ما رأوا أنه هجوم. فقد لاحظوا مسئولوا الشركة أن الموقع كان يعمل ببطء شديد عند افتتاح السوق وهو الأمر الذي أدى إلى انخفاض إمكانية الوصول إليه إلى 50٪.
راجع في ذلك D. voloninalinu ibid, p. 6

(3) انظر في ذلك:
Richard totta and antong hardcastle, computer related crime in information technology the law edited by chris Edwards and Nigel savage Macmillan publisher 1986,p.201

لارتكاب الجريمة في المعوقات التي يمكن أن تواجه في هذا المجال وهي:

- إما تجاهل هذا الدليل تماماً.
- إما محاولة فحص هذا الدليل بدون أية مهارات في مجال الكمبيوتر.
- إما حَمْل المشتبه فيه على استعادة معلومات من الكمبيوتر، ثم بعد ذلك عدم مصادرة نظام الكمبيوتر حيث أن الشهادة التي يدلي بها تصبح حرجة في مواجهة المعلومات المستمدة من الكمبيوتر.
- وإما مصادرة جهاز الكمبيوتر بدون معرفة ما يوجد فيه من معلومات وتالياً، زيادة الفرصة في فقد هذه المعلومات.

**3 ـ إحجام المجني عليهم عن التبليغ:**

ويعدّ هذا الأمر على قدر من الصعوبة، لا في مجال اكتشاف وإثبات جرائم الحاسب، بل وفي دراسة هذه الظاهرة برمّتها وهو ما يُعبَّر عنه بالرقم الأسود[1]. لجرائم الحاسب.

(1) ويلاحظ في هذا الشأن أن المشرّع الإماراتي جعل الإبلاغ عن الجرائم إلزامياً كقاعدة عامة وإلا تعرض المخالف للجزاء الجنائي، إذ أوجب لمقتضى المادة (37) من قانون الإجراءات الجزائية رقم 35 لسنة 1992، وعلى كل من علم بوقوع جريمة مما يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب، أن يبلغ النيابة العامة أو مأموري الضبط القضائي عنها، ونص في المادة (38) من القانون ذاته على أنه يجب على كل من علم من الموظفين العموميين أو المكلفين بخدمة عامة أثناء تأدية عمله أو بسبب تأديته، بوقوع جريمة من الجرائم التي يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب، أن يبلغ عنها فوراً النيابة العامة أو أقرب مأموري الضبط القضائي ورصد مخالفة هذا الواجب عقوبة جنائية ينصّها في الفقرة الثانية من المادة (272) من قانون العقوبات الاتحادي على «أن. . . يعاقب بالغرامة كل موظف غير مكلف بالبحث عن الجرائم، أو ضبطها أهمل أو أرجأ إبلاغ السلطة المختصة بجريمة علم بها في أثناء أو بسبب تأديته وظيفته ولا عقاب إذا كان رفع الدعوى. . معلقاً على شكوى. . . كما جاءت المادة (274) من القانون ذاته لتقضي بأن يعاقب بغرامة لا تجاوز ألف درهم كل من علم بوقوع جريمة وامتنع عن إبلاغ ذلك إلى السلطات المختصة، ويجوز الإعفاء من هذه العقوبة إذا كان من امتنع عن الإبلاغ زوجاً لمرتكب الجريمة أو من أصوله أو فروعه أو أخوته أو إخوانه أو من هم في منزلة هؤلاء من الأقرباء بحكم المصاهرة.

وفى هذا الشأن يحدثنا Beter swift : يعتقد اتحاد الصناعة البريطاني «confederation of britich industry» أن العديد من الشركات تحرّج من الاعتراف بأنها تعرضت للسلب، حسب تعبيره، من قبل مجرمى التقنية العالمية فبدلاً من استدعاء الشرطة والاعتراف بأنهم ضحايا جرائم السرقة فإنهم يخلدون إلى الصمت[1].

ويلاحظ أن العديد من ضحايا جرائم الحاسب لا يقفون عند حد عدم الإبلاغ عن الجريمة، بل إنهم يرفضون أي تعاون مع الجهات الأمنية خشية معرفة العامة بوقوع الجريمة، ويسعون بدلاً من ذلك إلى محاولة تجاوز آثارها حتى لو كانت الوسيلة هى مكافأة المجرم. ونذكر على سبيل المثال واقعة بنك Marchant bank city في انجلترا لنقل 8 مليون جنيه استرلينى من أحد أرصدته إلى رقم حساب في سويسرا، وقد تم القبض على الفاعل أثناء محاولته سحب المبلغ المذكور، ولكن بدلاً من أن يقوم البنك بتحريك الدعوى الجنائية ضده فقد قام بدفع مبلغ 1 مليون جنيه استرلينى له بشرط عدم إعلام الآخرين عن جريمته وإخطار البنك بالآلية التي نجح من خلالها باختراق نظام الأمن الخاص بحاسب البنك الرئيسي[2].

وفى دراسة أجريت عام 1980 في فرنسا أشارت النتائج إلى أن جرائم الحاسب التي تمّ الإبلاغ عنها للسلطات الخاصة بلغت 15٪ من مجموع الجرائم وأن ادلة الإدانة لم تتوافر إلا بنسبةٍ تقدر بحوالى خُمْس النسبة المتقدمة، أي ما يعادل حوالى 3٪من مجموع جرائم الحاسب المرتكبة.

كما تؤكد دراسة حديثة أجريت في الولايات المتحدة الامريكية أن الرقم

---

(1) انظر في ذلك :
Peter swift Hackmun - menace of the key board criminal brithish telecom world mag half of sep. 1989,p.13-14

(2) راجع في ذلك : Peter swift Hackan, ibid, p. 3

الأسود لجرائم الحاسب يميل إلى الارتفاع. فاستناداً إلى تحليل الباحثين، وفي ضوء تقارير جمعيات صانعى الحاسبات، يظهر أن الرقم الأسود ما يقارب نسبة 60٪ من جرائم الحاسب[1].

**4 ـ دور الخبراء في فحص البيانات:**

يشكل الكمّ الهائل للبيانات التي يتم تداولها من خلال الأنظمة المعلوماتية أحد مصادر الصعوبات التي تعوق تحقيق الجرائم التي تقع عليها أو بوساطتها، والدليل على ذلك أن طباعة كل ما يوجد على الدعامات الممغنطة لمركز حاسب متوسط الأهمية يتطلب مئات الآلاف من الصفحات والتى قد لا تُثبت كلها تقريباً شيئاً على الإطلاق. ويسلك المحقق غير المدرب لمواجهة هذه الصعوبة أحد سبيلين:

إما حجز البيانات الإلكترونية بقدر يفوق القدرة البشرية على مراجعتها، أو التغاضي عن هذه البيانات كلها على أمل الحصول على اعتراف بالجريمة من المتهم[2].

الواقع أنه بالامكان مواجهة هذة الصعوبة عن طريق أحد أمرين:

أ ـ الاستعانة بالخبرة الفنية لتحديد ما يجب، دون سواه، البحث عنه للإطلاع عليه وضبطه واستعانة الجهات القائمة بالتحري والتحقيق، والحكم بالخبراء حين تتعامل مع الجرائم التي تقع في مجال تكنولوجيا المعلومات تكاد تكون ضروره لاغنى عنها نظراً للطابع الفني الخاص لأساليب ارتكابها، والطبيعة المعنوية لمحل الاعتداء، ونجاح هذه الجهات في أداء

(1) راجع في ذلك:
يونس خليل عرب مصطفى، جرائم الحاسب ـ دراسة مقارنة رسالة ماجستير ـ مقدمة إلى كلية الدراسات العليا الجامعة الأردنية، 1994، ص73.

(2) راجع في ذلك: د. هشام محمد فريد رستم سبقت الإشارة إليه، ص37.

رسالتها يتوقف إلى حد كبير، علاوةً على حسن اختيار الخبير، على نجاحه في المهمة التي عهد إليه بأدائها وموضوع هذه المهمة، وإن كان يمكن للخبير نفسه أن يحدده إلا أن ذلك ليس مرغوباً فيه تجنباً لهيمنة دور الخبير على العملية الإثباتية وطغيانه على دور المحقق أو القاضي.

ب ـ الاستعانة بما تتيحه نظم المعالجة الآلية للبيانات من أساليب للتدقيق والفحص المنظم أو المنهجي ونظم ووسائل الاختبار والمراجعة.

## المعوقات الخاصة بالتنسيق الدولي في مجال جمع الأدلة

من خصائص جرائم الحاسب أنها جرائم عابرة للحدود الوطنية، أو الإقليمية أو القارية، وأن مواجهتها على نحو مؤثر، يتطلب العمل من خلال محورين:

الأول : سَنّ النصوص الجنائية الموضوعية على الصعيد الوطنى لتجريم صورها المختلفة والعقاب عليها، إضافة إلى سن قواعد جنائية إجرائية تتلاءم مع خصائصها وطبيعتها المميزة. وثانيهما: خلق وتطوير وإنماء العمل الدولي المشترك لمواجهة هذه الظاهرة من خلال وضع حلول للمشاكل التي تحد من فاعلية مكافحتها، سواءٌ المشاكل الناجمة عن تطبيق القواعد الموضوعة، أو القواعد الاجرائية على هذا النمط المستحدث من الجرائم.

وهناك عقبات عديدة تقف كحجر عثرةٍ من أجل التنسيق الدولي في مكافحة جرائم سرقة المعلومات وأبرزها ما يلى:

1 ـ عدم وجود مفهوم عام مشترك بين الدول حتى الآن حول نماذج النشاط المكوّن للجريمة المتعلقة بالحاسب الآلي.

2 ـ عدم وجود تعريف قانوني موحد للنشاط الإجرامي المتعلق بهذا النوع من الإجرام.

3 ـ اختلاف مفهوم الجريمة لاختلاف التقاليد القانونية وفلسفة مختلف النظم القانونية.

4 ـ انعدام التنسيق بين قوانين الإجراءات الجنائية للدول المختلفة فيما يتعلق بالتحري والتحقيق في الجريمة المعلوماتية.

5 ـ تعقد المشاكل القانونية والفنية الخاصة بتفتيش نظم المعلومات خارج حدود الدولة أو ضبط معلومات مخزنة فيه أو الأمر بتسليمها.

6 ـ عدم وجود معاهدات للتسليم أو للتعاون الثنائي أو الجماعي بين الدول تسمح بالتعاون الدولي أو عدم كفايتها إن وجدت لمواجهة المتطلبات الخاصة للجرائم المعلوماتية وسرعة التحريات فيها(1).

(1) لمواجهة هذه المشكلات أو بعضها، ناشد مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين والذي عقد في هافانا عام 1990 في قراره المتعلق بالجرائم ذات الصلة بالحاسب، الدولَ الأعضاءَ أن تكثف جهودها كي تكافح بمزيد من الفعاليات عمليات إساءة استعمال الحاسب التي تستدعي تطبيق جزاءات جنائية على الصعيد الوطني بما في ذلك النظر إذا دعت الضرورة في أ ـ تحديث القوانين والإجراءات الجنائية بما في ذلك اتخاذ تدابير من أجل:

1 ـ ضمان أن الجزاءات والقوانين الراهنة بشأن سلطات التحقيق وقبول الأدلة في الاجراءات القضائية تنطبق على نحو ملائم وإدخال تغييرات مناسبة عليها إذا دعت الضرورة لذلك.

2 ـ النص على جرائم وجزاءات إجراءات تتعلق بالتحقيق والأدلة حيث تدعو الضرورة إلى ذلك للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي في حالة عدم وجود قوانين تنطبق على نحو ملائم. كما حث المؤتمر كذلك الدول الاعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالحاسبات بما في ذلك دخولها، حسب الاقتضاء، أطرافا في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدات في المسائل الخاصة المرتبطة بالجرائم ذات الصلة بالحاسب. ونَصح القرار ذاته الدول الأعضاء بالعمل على أن تكون تشريعاتها المتعلقة بتسليم المجرمين وتبادل المساعدة في المسائل الجنائية منطبقة انطباقاً كافياً على الأشكال الجدية للإجرام، مثل الجرائم ذات الصلة بالحاسب، وأن تتخذ خطوات محددة، حسب الاقتضاء من أجل تحقيق هذا الهدف، وذلك بالإضافة إلى توصيات أخرى وقد يكون ملائماً كخطوة تعزز مسار التعاون الفعال وتكمل ما اتخذه مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين في هذا الشأن من قرارات أن يسفر بحث مؤتمرات الأمم المتحدة لموضوع الجرائم ذات الصلة بالحاسب عن فتح آفاق جديدة للتعاوقن الدولي في

## المبحث الثالث:
## دور التعاون الدولي في مجال مكافحة جرائم المعلوماتية والإنترنت

أصبح لكل شخص يعيش في المجتمع الحق بالاتصال بغيره وتبادل المنافع المعنوية والمادية معه، ليس فقط داخل دولته بل كذلك خارجها مع أبناء الدول الأخرى.

وإذا كانت الدول قد استطاعت الحدّ من ذلك الاتصال والتبادل في أوقات مضت تحت ستار حماية متطلبات أمنها القومي والاقتصادي إلا أنها لم تعد كذلك في ظل عصر السماوات المفتوحة بفعل تقدم وسائل الاتصال عبر الأقمار الصناعية[1] ووسائط نقل الأخبار المعلوماتية ـ عبر الأثير والموجات الكهرومغناطيسية لدرجة يمكن القول معها أن سيادة الدولة الإقليمية قد انحسرت عن الإقليم الفضائي، أو الهوائي، واقتصرت على إقليمها الأرضي والمائي فقط[2].

= هذا المضمار لا سيما فيما يتعلق بوضع أو تطوير: أ – معايير دولية لأمن المعالجة الآلية للبيانات. ب – تدابير ملائمة لحل مشكلات الاختصاص القضائي التي تثيرها الجرائم المعلوماتية العابرة للحدود أو ذات الطبيعة الدولية. جـ – اتفاقيات دولية تنطوي على نصوص تنظم اجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها والأشكال الأخرى للمساعدة المتبادلة مع كفالة الحماية في الوقت نفسه لحقوق وحريات وسيادة الدول.

راجع في ذلك : د. هشام محمد فريد رستم، سبقت الإشارة، ص 49

(1) راجع في ذلك :

Ravillon (Hume) les telecommunications par sateliet aspects juridiques Paris, ed, lifec 1997,

Mateesco - Matte (N) droit aerospatical les telcomunnications par natellites Pars, 1982

(2) راجع في ذلك Park 9K-G) la protection de la souverainet aerienne Paris, 1977 =

وقد كرست الأعمال القانونية الدولية حق الاتصال والحصول على المعلومات وتداولها، وأكدت على أهمية ضمان ممارسته[1].

فقد نصّ القرار 59 الصادر عن الأمم المتحدة في 14 ديسمبر/ أيلول 1946 على أن «حرية الاستعلام هي حق أساسي للإنسان، وهي حجر الزواية لكل الحريات التي كرست الأمم المتحدة نفسها للدفاع عنها، وحرية الاستعلام تشمل جمع ونقل ونشر المعلومات في كل دولة دون عقبات».

كما نصّت المادة 19 من الإعلان العالمي لحقوق الإنسان الصادر عن الجمعية العامة للأمم المتحدة في 10 ديسمبر 1948 على أن «لكل فرد الحق في حرية الرأي والتعبير، ويشمل هذا الحق حرية اعتناق الآراء دون تدخل واستقاء وتلقي وإذاعة الأنباء والأفكار دون تقيد بالحدود الجغرافية وبأية وسيلة كانت».

وأخيرا نصّت المادة 19 من العهد الدولي للحقوق المدنية والسياسية الصادر عن الأمم المتحدة في 16 ديسمبر 1966 على أن «2 ـ لكل فرد الحق في حرية التعبير وهذا الحق يشمل حرية البحث عن المعلومات أو الأفكار من أي نوع واستلامها ونقلها بغض النظر عن الحدود، وذلك إما شفاهةً أو كتابةً أو طباعةً، وسواءٌ كان ذلك في قالب فني أو بأية وسيلة أخرى يختارها».

وتنشأ ضرورة وجود توافق دولي محكم في مجال الحق في المعلومات على وجه الخصوص، من سهولة حركة المعلومات في أنظمة تقنية المعلومات حيث يرجع لهذه السهولة في حركة المعلومات أنه بالإمكان ارتكاب جريمة عن طريق حاسب آلي موجود في دولة معينة بينما يتحقق نجاح هذا النشاط الإجرامي في دولة أخرى.

---

(1) راجع في ذلك :
Pinto ® la Liberte d'infromation ed d'opinion en droit international, paris, L.G.D.J. 1984

وتستلزم مثل هذه الجرائم وجود تعاون دولي فعّال [1] والذي يعتبر ضرورياً من أجل حماية حقيقية لأنظمة الاتصالات البُعدية التي تمر بالعديد من الدول وينشأ حتماً عن وجود أوجه خلاف بين القوانين الوطنية والخاصة بتقنية نظم المعلومات ما يعرف بالمعلومات المختبئة والذي ستكون لها نتيجة عكسية في صورة قيود وطنية على حرية حركة المعلومات.

وفي مجال الاجراءات فإن التوافق بين مختلف سلطات التدخل الوطنية سيكون هاماً من أجل التيسير دون عقبة لطلب المساعدة القانونية الوطنية،أنه قد تلتمس إحدى الدول المساعدة القضائية من دولة أخرى، بحيث يمكن لهذه الأخيرة أن تباشر التدابير التي تكون طبقاً لقوانينها الخاصة.

## أولاً: التدابير الواجب مباشرتها على المستوى الوطني

يمكن تقسيم هذه التدابير إلى نوعين؛ أحدهما تدابير موضوعية والآخر إجرائية. وسنخصص لكل منهما مطلباً مستقلاً وذلك على النحو التالي :

### التدابير الموضوعية[2]

ينبغي على الدول أن تتبع سياسة جنائية مشتركة تهدف إلى حماية المجتمع من مخاطر الجريمة المعلوماتية، وذلك من خلال تبنى التشريعات الملائمة لمواجهة الخطورة المتمثلة في إمكان استخدام شبكات الكمبيوتر والمعلومات

(1) LA COmmision «invite fnstatment les autorites nationals compptentes a cooperer apin de parvenir a un accord international definissant les contenus illegaux et, par consequent, passibles de sanctions quelques soit le lieu de residence du fournisseur de contenu» et «propose Hume'etablissement de catalogues «nationaux» aisement accessibles recensant les contmis ou les operations illegales detectees sur intenrt».

راجع في ذلك : La criminamite infromatique sur L'internet

(2) راجع في ذلك

European committee on crime problems 9cppc). Committee of experts on crime in cyber - space (pc-cy) draft convention on cybercirm 9draf N19) stansbourg, 25 April 2000

الإلكترونية في ارتكاب أفعال إجرامية مع إمكانية تخزين ونقل الدليل المتعلق بمثل هذه الأفعال عبر تلك الشبكات.

لذا من الأهمية بمكان مباشرة التدابير الآتية :

**أولاً** : يجب على الدول كافة أن تتبنى التشريعية وغيرها من التدابير اللازمة لإدراك عملية الدخول غير المشروع إلى سائر أو جزء من أجزاء نظام الكمبيوتر كجريمة جنائية وفقاً لأحكام قوانينها الوطنية إذا ما ارتُكِبت هذه الأفعال بصورة عَمْدية، ويجوز لأي دولة أن تحدد من بين متطلبات ارتكاب الجريمة أن يكون ارتكابها من خلال اختراق تدابير الأمن أو بنيَّة الحصول على بيانات الكمبيوتر.

**ثانياً** : ينبغي أن تتبنى التدابير التشريعية وغيرها من التدابير اللازمة لإدراك أعمال الاعتراض دون حق والتي تتم بأساليب فنية، كعمليات نقل الكمبيوتر إلى، أو من خلال، حاسب آلي آخر، وكذا الإشارات الالكترومغناطيسية الصادرة من أحد نظم المعلومات والتي تحمل مثل تلك البيانات واعتبارها جريمةً جنائيةً لأحكام قوانينها الوطنية إذا ما ارتكبت بصورة عمدية.

**ثالثاً**: يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإدراك أعمال الإضرار، أو المحو، أو الإتلاف، أو التعديل، أو الإعاقة التي تستهدف بيانات الحاسب الآلي بدون وجه حق واعتبارها جريمة إذا ما ارتُكِبت بصورة عمدية.

**رابعاً**: يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإدراج أعمال الإعاقة الخطرة دون وجه حق بوظائف نظام الكمبيوتر من خلال إدخال أو نقل أو الإضرار أو محو أو إتلاف أو تعديل أو إعاقة بيانات الكمبيوتر وإدراكها باعتبارها جريمة جنائية إذا ارتُكِبت بصفة عمدية.

**خامساً** : يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإمكانية مُساءلة الأشخاص المعنوية جنائياً عن الجرائم الناشئة عن نظم المعلومات وذلك

في الأحوال التي يؤدي فيها قصور الإشراف أو الرقابة الطبيعية من قبل الشخص إلى تسهيل ارتكابها.

**التدابير الاجرائية[1]**

وتتمثل هذه التدابير على النحو التالي:

**أولاً**: يجب على الدول أن تتخذ التدابير التشريعية التي تخولها سلطة تفتيش:

أ - أحد أنظمة الكمبيوتر أو جزء منه وبيانات الكمبيوتر المختزنة به.

ب - أحد الوسائط التي قد تكون بيانات الكمبيوتر مختزنةٌ به، وذلك في أراضيها أو في أحد الأماكن الأخرى التي تمارس عليها سلطاتها لأغراض التحقيق.

**ثانياً**: يجب على الدول أن تتخذ التدابير التشريعية اللازمة لتخويل سلطاتها المعنية في إصدار الأمر لأي شخص سواءٌ كان موجوداً في إقليمها في أي مكان آخر عليه سلطاتها السيادية، لكي يقدم أية بيانات محددة واقعة تحت سيطرته ومخزّنة في أحد أنظمة الكمبيوتر أو أحد الوسائط المستخدمة في تخزين البيانات وذلك بالصورة التي تطلبها تلك السلطات لأغراض التحقيق.

**ثالثاً**: يجب على الدول أن تتبنى التدابير التشريعية اللازمة لتمكين سلطاتها المعنية من الحصول على نسخة حفظ سريعة للبيانات المخزنة في أحد نظم الكمبيوتر، وذلك لأغراض التحقيقات، إذا تبين أنها معرضة بصفة خاصة للفقد والتعديل.

**رابعاً**: يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإجبار

(1) راجع في ذلك
Europan committee on crime problems (cppc) committee of experts on rime in cyber - space (pc - cy0 draft convention on cyber crimd (draft N 10) Strasbourg 25 april 2000

الشخص الذي تتخذ حياله إجراءات الحفظ المشار إليها سلفاً على الاحتفاظ بسرية الإجراءات لمدة محدّدة من الزمن، وفقاً للإطار الذي يسمح به القانون الوضعي.

**خامساً**: يجب على الدول أن تتخذ التدابير التشريعية اللازمة التي تكفل حفظ بيانات النقل، والخاصة بأحد الاتصالات المحددة، كما تكفل الحفظ السريع لتلك البيانات الخاصة بعملية النقل وبغض النظر عمّا إذا كان مقدم الخدمة واحداً أو أكثر ممن شاركوا في عملية نقل هذا الاتصال.

**سادساً**: يجب على الدول أن تتخذ التدابير التشريعية اللازمة لمدّ اختصاصها القضائي على أي من الجرائم المشار إليها إذا ما ارتكبت:

أ ـ بصورة كليه أو جزئية على أراضيها أو على متن باخرة أو طائرة أو قمر صناعي يحمل علمها أو مسجل لديها.

ب ـ من قبل أحد مواطنيها إذا كانت الجريمة من الجرائم المعاقب عليها وفقا لأحكام القانون الجنائي الساري في محل ارتكابه أو إذا كانت الجريمة قد ارتكبت خارج الاختصاص الإقليمي لأي دولة.

## التدابير الواجب مباشرتها على المستوى الدولي[1]

ويمكن تقسيم هذه التدابير إلى نوعين: الأول؛ يتعلق بالتسليم والثاني: يتعلق بالمعونة المتبادلة.

### أ ـ تسليم المجرم المعلوماتي

يجب على الدول أن تتعاون، بعضُها مع بعض، ومن خلال تطبيق

(1) راجع في ذلك
Europan committee on crime problems (cppc) committee of experts on rime in cyber - space (pc - cy0 draft convention on cyber crimd (draft N 19) Strasbourg 25 april 2000

المواثيق الدولية ذات الصلة بشأن التعاون الدولي في المسائل الجنائية، وعلى وجه الخصوص في مجال تسليم المجرم المعلوماتي حيث يجب تسليم مرتكبيها وذلك وفقاً لمعيار معين لتكييف الجريمة كجريمة يجوز تسليم مرتكبيها:

- أن يكون الدخول إلى النظام أو البيانات قد تمّ بدون وجه حقٍ وبنيّة الإخلال بسرية البيانات أو إعاقة نظام الكمبيوتر.

**ثانياً** : أن تبرم الدول في ما بينها اتفاقية تسليم مرتكبي الجرائم المعلوماتية.

**ثالثاً** : إذا ما رُفض طلب التسليم الصادر في شأن مرتكبي إحدى الجرائم المعلوماتية بناءً على جنسية الشخص المراد تسلميه نظراً لأن طرف المدّعي يعتبر أنه يختص قضائياً بالجرمية محل الادعاء، يقوم الطرف المدَّعىٰ عليه بتقديم القضية إلى سلطاته بغرض السير في الدعوى الجنائية، وعلى أن يبلّغ الطرف المدعي بالنتائج المترتبة عليه.

**ب ـ المعونة المتبادلة**

وتتمثل المعونة المتبادلة في الإجراءات التالية :

**أولاً** : يجب على الدول أن تقدم بعضُها لبعضٍ المعونة المتبادلة وذلك بأكبر قدر ممكن، لأغراض التحقيق والإجراءات الخاصة بالجرائم الجنائية المتعلقة بنظم وبيانات الحاسب الآلي.

**ثانياً** : يجب على الدول أن تقبل وتستجيب إلى طلبات المعونة المتبادلة من خلال وسائل الاتصال السريعة كالفاكس والبريد الإلكتروني، بالقدر الذي يوفر للطرف الطالب المستوى من الأمن والمصداقية.

**ثالثاً**: تخضع المعونة المتبادلة للاشتراطات المنصوص عليها في قوانين الدولة المدعية أو المنصوص عليها بموجب اتفاقيات المعونة المتبادلة.

**رابعاً**: في الأحوال التي يُسمح فيها للطرف المُدّعىٰ عليه بتعليق طلب المعونة المتبادلة على اشتراط وجود جريمة مزدوجة، يعتبر هذا الشرط محلَّ

اعتبار وبغض النظر عما إذا كانت قوانين هذه الدولة تضع الجريمة في نطاق ذي تصنيفُ آخر.

**خامساً**: تحدد كل دولة سلطة مركزية تنهض بالمسؤولية لإرسال طلبات المعونة المتبادلة والرد عليها وتنفيذها أو نقلها للسلطات المعنية للتنفيذ.

**سادساً**: تنفذ طلبات المعونة المتبادلة وفقاً للإجراءات التي يحددها الطرف المدّعي فيما عدا الأحوال التي لا تتصل فيها تلك الاجراءات مع أحكام القانون السائد بالدولة المعتدى عليها.

**سابعاً**: يجوز للدولة المُدّعىٰ عليها أن ترفض طلب المعونة إذا ما توافرت لديها القناعة بأن الالتزام بما ورد بالطلب قد يخلّ بسيادتها أو أمنها أو نظامها العام أو بأي من مصالحها الأساسية الأخرى.

**ثامناً**: يجوز للدولة المُدّعىٰ عليها تأجيل التصرف في الطلب إذا كان هذا التصرف سيخلّ بالتحقيقات أو إجراءات الآدّعاء أو الاجراءات الجنائية التي تباشَر بمعرفة السلطات المعنية.

**تاسعاً**: يجب على الدول المُدّعى عليها أن تُخطِر الدولة المدعية بصورة فورية بنتائج تنفيذ طلب المعونة، فإذا ما رُفض الطلب أو تمّ تأجيله يجب تقديم الأسباب سواء للرفض أو التأجيل.

**عاشراً**: يجوز للدولة المدعية أن تطلب من الدولة المُدّعىٰ عليها أن تحتفظ بسرية الوقائع والمحتويات التي يتضمنها الطلب، فإذا لم يكن بمقدور الدولة المدعية عليها الوفاء بمتطلبات سرية الطلب فيجب عليها إخطار الدولة المدعية بذلك، وعلى الأخيرة في هذه الحالة تحديد ما إذا كان سينفذ الطلب من عدمه.

**أحَدَ عشر**: يجوز في حالة الاستعجال إرسال طلبات المعونة المتبادلة مباشرة إلي السلطات القضائية بما فيها النيابة العامة لدى الدولة المدّعية عليها،

وفي مثل هذه الحالة يجب إرسال نسخة بالطلب نفسه إلى السلطة المركزية القائمة لدى الدولة المُدّعىٰ عليها.

## الإجراءات الوطنية والدولية لمواجهة جرائم الكمبيوتر:

**أ ـ المستوى الوطني :**

نظراً لظهور مشكلة جرائم الكمبيوتر كمشكلة أمنية، وقانونية واجتماعية، فإن خبراء الأمن المعلوماتي وصانعي السياسات الحكومية ومسوِّقي الكمبيوتر، والأفراد المهتمين في هذا الموضوع، بحاجة إلى تغيير نظرتهم تجاه جرائم الكمبيوتر، لا لأنها مشكلة وطنية فقط، وإنما كمشكلة عالمية،وتتطلب الإجراءات الوطنية تعاوناً في مجال القطاعين العام والخاص،فعلى القطاع الخاص الالتزام بإجراءات الوقاية، وعلى القطاع العام تنفيذ الإجراءات اللازمة لمكافحة الجريمة،وبوجه عام هناك حاجة إلى تحقيق ما يلي:

1 ـ إيجاد التشريعات اللازمة لحماية ملكية الكمبيوتر، والبيانات، والمعلومات والمعدات اللازمة للتشغيل والتوصيل.

2 ـ زيادة الوعي الوطني بجرائم الكمبيوتر والعقوبات المترتبة عليها.

3 ـ إنشاء وحدات مختصة في التحقيق في جرائم الكمبيوتر في المحاكم والشرطة.

4 ـ إيجاد نوع من التعاون مع الدول الأخرى في الحماية والوقاية من هذه الجرائم.

**ب ـ المستوى العربي:**

عقدت الجمعية المصرية للقانون الجنائي مؤتمرها السادس في القاهرة في الفترة من 25 إلى 28 أكتوبر/ت[1] 1993م وناقشت موضوع جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، من خلال الأبحاث

والدراسات المقدمة من الباحثين والتي دارت حول تحديد مختلف أنواع الجرائم المتعلقة بنظم المعلومات من اعتداء مادي على الأجهزة وأدوات الكمبيوتر بالسرقة أو التخريب أو الإتلاف، إلى اعتداء على البيانات والمعلومات المختزنة في قواعد المعلومات بالغش أو التزوير أو السرقة، والحصول على تلك البيانات والمعلومات من دون إذن أو الاتجار فيها، والتحايل على الأجهزة للحصول على الأموال، وتحويل ونقل الأموال المتحصلة من الجرائم لغسلها.

وأوضحت البحوث والمناقشات أن الاعتداء قد يحدث أثناء إدخال البيانات والمعلومات أو إخراجها أو من خلال المعالجة الآلية لها، وذلك بالحذف أو المحو أو الإضافة أو التعديل دون وجه حق، وأن هذه المعلومات قد تكون ثقافية أو سياسية أو عسكرية أو اقتصادية أو علمية أو اجتماعية. وقد بينت الأبحاث والدراسات والمناقشات صعوبة اكتشاف جرائم نظم المعلومات وإثباتها، وأكدت على ضرورة تدريب رجال الشرطة القضائية ورجال التحقيق ورجال القضاء، كما حذرت من تزايد احتمالات انتهاك حرمة الحياة الخاصة عن طريق التجسّس والتنصت على الكابلات الرابطة بين القواعد الأساسية والوحدات الفرعية.

وفي ختام المؤتمر، تمكن المؤتمرون من تجريم الأفعال المتعلقة بالكمبيوتر والتوصية باتخاذ التدابير والإجراءات اللازمة والتي تكون على النحو التالي:

- **تجريم الأفعال المتعلقة بالكمبيوتر:**

1 ـ حصول الشخص لنفسه أو لغيره على أموال عن طريق اختراق نظم المعلومات للاستيلاء علبها دون وجه حق.

2 ـ حصول الشخص لنفسه أو لغيره على بيانات أو معلومات أو مستندات عن طريق اختراق نظم المعلومات من دون إذن.

3 ـ حصول الشخص لنفسه أو لغيره على أموال دون وجه حق عن طريق التحايل على الأجهزة.

4 ـ تحويل أموال دون وجه حق عن طريق اختراق الأجهزة.

5 ـ تحويل أموال مستمدة بطريق غير مشروع عن طريق الأجهزة بقصد غسلها وتمويه مصدرها.

6 ـ إتلاف أو تشويه البيانات أو المعلومات أو المستندات المختزنة في قاعدة المعلومات.

7 ـ استخدام المعلومات المختزنة في قاعدة نظم المعلومات بقصد المساس بحرمة الحياة الخاصة للغير أو حقوقهم.

8 ـ تغيير الحقيقة في البيانات أو المعلومات أو المستندات التي تحويها قاعدة نظم المعلومات عن طريق الإضافة أو الحذف أو المحو الكلي أو الجزئي أو التعديل.

9 ـ حصول الشخص على نسخة من البرامج المختزنة في قاعدة نظم المعلومات من دون إذن.

10 ـ حصول الشخص على البيانات أو المعلومات أو المستندات التي تحويها قاعدة نظم المعلومات بقصد إفشائها أو قيامه بإفشائها فعلا أو الانتفاع بها بأي طريق.

11 ـ الاطلاع بأي طريق على المعلومات أو البيانات أو المستندات التي تحويها قاعدة نظم المعلومات دون إذن بقصد معرفتها.

12 ـ التسبّب خطأً في حصول الغير على أموال أو بيانات أو معدات أو معلومات أو مستندات أو في ارتكاب فعل من الأفعال المذكورة أعلاه.

● **الإجراءات والتدابير الواجب اتباعها:**

1 ـ مساءلة الأشخاص الطبيعيين والأشخاص المعنويين والمؤسسات الفردية إذا اقترنت الجريمة لصالح الأشخاص والمؤسسات أو بأسمائها بالإضافة إلى مساءلة الأشخاص الطبيعيين من مقترفيها وشركائهم.

2 ـ إدماج نصوص جرائم نظم المعلومات في قانون العقوبات الوطني على أن يفرد لها فصل خاص.

3 ـ تدريب رجال الشرطة القضائية ورجال التحقيق والقضاء على كيفية استخدام أجهزة المعلومات وأدواتها وأشرطتها وآلات الطباعة الخاصة بها والإحاطة بكيفية إساءة استخدامها.

4 ـ تدريب رجال الشرطة القضائية والتحقيق والقضاء على كيفية الكشف عن هذه الجرائم وإثباتها.

5 ـ حث الدول على التعاون فيما بينها، بخاصة في مجال المساعدات والإنابة القضائية للكشف عن هذه الجرائم، وجمع الأدلة لإثباتها، وتسليم المجرمين الذين اقترفوها، وتنفيذ الأحكام الأجنبية الصادرة بالإدانة والعقوبة على رعايا دولة مقترفيها إياها في الخارج.

ومن جانب آخر تعكف جامعة الدول العربية ممثلة في الأمانة العامة لمجلس وزراء الداخلية العرب على إعداد مشروع اتفاقية عربية لجرائم الكمبيوتر وكذلك إنشاء لجنة تتألف من ممثلي عدد من الدول الأعضاء لمتابعة المستجدات التقنية والاتفاقيات الدولية كافة المتعلقة بجرائم الكمبيوتر والعمل على توحيد التشريعات العربية بهذا الشأن.

**ج ـ المستوى الدولي:**

الجرائم المتعلقة بالكمبيوتر تتضمن موقفاً متحولاً أو متنقلاً، أو متحركا وذلك بسبب طبيعة الكمبيوتر، فان إمكانية التخزين متزايدة وكذلك

التحريك،وانتقاء البيانات من خلال الاتصال من مسافة بعيدة،والقدرة على الاتصال ونقل البيانات وتحويلها بين الكمبيوتر من مسافات كبيرة. وكنتيجة لذلك فإن عدد الأمكنة والدول التي يمكن أن تكون متورطة في حالات جرائم الكمبيوتر في تزايد. وقد ترتكب الجريمة في نظام عدلي معين وجزئياً في نظام ثانٍ وثالثٍ ومن أي مكان في العالم.

ومع خاصّة الحدّ المتحرك فإنه لا بد من تحديد مكان وقوع الجريمة حيث أن أي نظام قضائي يجب أن يتعامل معها (التحقيق والمحاكمة). أما إذا كانت الجريمة تتطلب تدخل دولتين فان تصارع الأنظمة القضائية أمر وارد، إذا لم يكن هناك اتفاقيات ثنائية أو قانون دولي تلتزم به الأطراف المعنية.

ويرتبط مع مشكلة الحد المتحرك، مشكلة تتعلق بسيادة الدولة في سن التشريعات للأفعال التي تحصل على أراضيها،والسؤال هنا كيف يتحدد مكان الجريمة؟ فبعض الدول ترى أن مكان ارتكاب الجريمة يمكن تحديده على مبدأ الوجود في الوقت ذاته، حيث يمكن تحديد مكان جريمة بناءً على حدوثها في مكان ما أو جزء منها.

أما المبدأ الثاني في تحديد الجريمة فيعتمد على مكان الأثر،فالمكان الذي يظهر فيه أثر الجريمة يعدّ مكان ارتكابها، وهذا المبدأ مقبول في دول كثيرة، بخاصة الأوروبية. وهنا تصبح جرائم الكمبيوتر ذات صلة.(فالفرد الذي يضغط على لوحة مفاتيح الكمبيوتر في بلد (أ) يمكن أن يدخل على بيانات في بلد (ب) ويمكن أن يحولها إلى بلد (ج)، مثل تحويل العملات أو الحوالات المالية.

وتظهر مشكلة أخرى وهي تتعلق بالسلوكيات المنحرفة في الجرائم ذات الصلة بالكمبيوتر، وهي تتعلق باستخدام فيروسات الكمبيوتر، فإذا تمكن شخص ما من دخول قاعدة البيانات لأحد البنوك، وغذاها بأحد الفيروسات، وكان هذا الفيروس مبرمجاً بحيث ينقل نفسه إلى بلاد أخرى، أو مدن أخرى.

وعندما يدمر الفيروس برنامج أحد البنوك، فان الأثر الناجم عن ذلك

يظهر في أكثر من دولة، فأيٌّ من هذه الدول لها حق التحقيق والحكم في هذه الجريمة؟ إن مكان الجريمة هو مكان استخدام الكمبيوتر في تنفيذ العملية (بلد ـ أ) أم البلد الذي تحولت إليه البيانات (بلد ـ ب)، والمبدأ الأكثر تطبيقاً فيما يتعلق بالجرائم المتصلة بالكمبيوتر يقود إلى نتيجة مفادها أن مكان جريمة الكمبيوتر يتحدد في المكان الذي حصل فيه أحد أجزاء هذه الجريمة، وهذا يتطلب تنسيقاً دولياً بين مختلف أنظمة العدالة فيما يتعلق بالمحاكمة، والعقوبة. . . .

والأساس الآخر يكمن في تطبيق القانون في حالات العناصر الموجودة خارج حدود الدولة، فيما يتعلق بالاحتيال، والتخريب، والاستخدام غير المشروع. . . بوساطة الكمبيوتر أو للمعلومات الموجودة فيه. والموضوع المشار إليه هنا هو تأمين الحماية لبعض أنواع التعديات والجرائم المتصلة بالكمبيوتر في مواضيع الاقتصاد، أو البيانات الحكومية. . . والحكومات توسع نطاق نظامها العدلي إلى خارج حدودها لحماية أمنها الداخلي.

أما مشكلة الدخول المباشر حيث التقنيات الحديثة جعلت من الممكن أن تكون البيانات متوافرة في بلد ما بينما هي مخزنة في بلد آخر، فهذا الموقف أصبح منتشراً، خصوصاً في شبكات المعلومات الدولية. وهناك من يرى أن الدخول لقواعد المعلومات الوطنية من خارج الحدود الجغرافية يعد تدخلاً في استقلالية الدولة وسيادتها.

وبما أن العالم مترابط إلكترونياً، فيجب الاهتمام على المستوى الدولي بمشكلة جرائم الكمبيوتر، وبخاصةٍ في مجال التشريعات والتعاون المتبادل، ويعتقد مركز الأمم المتحدة للتطوير الاجتماعي والشؤون الإنسانية أن الوقاية من جرائم الكمبيوتر تعتمد على الأمن في إجراءات معالجة المعلومات، والبيانات الإلكترونية، وتعاون ضحايا جرائم الكمبيوتر،ومنفذي القانون، والتدريب القانوني، وتطور أخلاقيات استخدام الكمبيوتر.والأمن الدولي لأنظمة

المعلومات. ففي المجال الدولي هناك حاجة للتعاون المتبادل بين الدول، والبحث الجنائي والقانوني فيما يتعلق بهذا العالم الجديد الذى يحتاج منا المزيد من الجهد لسبر أغواره والتعمق فيه أموره؛ فعلى سبيل المثال، قدمت لجنة جرائم الكمبيوتر في الاتحاد الأوروبي توصيات تتعلق بجرائم الكمبيوتر تمحورت في النقاط التالية:

1 ـ المشكلات القانونية في استخدام بيانات الكمبيوتر والمعلومات المخزنة فيه في التحقيق الجنائي.

2 ـ الطبيعة العالمية لبعض جرائم الكمبيوتر.

3 ـ تحديد معايير لوسائل الأمن المعلوماتي وللوقاية من جرائم الكمبيوتر.

4 ـ مشكلة الخصوصية وخرقها في جرائم الكمبيوتر.

5 ـ موقف ضحايا جرائم الكمبيوتر.

6 ـ إدراك أهمية الاستجابة الدقيقة والسريعة للتحدي الجديد للجرائم المتصلة بالكمبيوتر.

7 ـ أن يؤخذ بالحسبان أن الجرائم المتصلة بالكمبيوتر ذات خاصية تحويلية.

8 ـ الوعي بالحاجة الناجمة للتناغم بين القانون والتطبيق وتحسين التعاون الدولي القانوني.

# خاتمة الدراسة

تحدثنا في هذه الدراسة عن جرائم المعلوماتية والانترنت (الجرائم الرقمية) في الإمارات ومصر والوطن العربي، مع إشارة لبعض الحالات التطبيقية من غير الدول العربية. وتهدف الدراسة إلى معرفة الجرائم التي ترتكب على الكمبيوتر كجهاز مادي والجرائم الإلكترونية والمعلوماتية الأخرى. وغنيّ عن البيان أن جرائم الإنترنت قد لاقت ذيوعاً وانتتشاراً كبيراً في السنوات الأخيرة مما ترتب عليه العديد من الأضرار والمساوىء التي عانى منها الأفراد والمؤسسات بل والحكومات التي تدير شؤون هؤلاء الأفراد.

ويجب التأكيد على أن الجريمة الإلكترونية، ليست حكرا على بعض الدول دون الآخر، فاللافت أن الواقع الذى يفرضه التقدم التكنولوجى والمعلوماتي، يؤكد أن هذه الجريمة الجديدة، آخذة في الانتشار، حيث إننا نجد محترفى إجرام المعلومات والإنترنت منتشرين في العالم العربى عامة، وفي مصر خاصة، رغم أنها لا تُعد من الدول المتقدمه بأي حال، ناهيكم عن أن الدول الأوروبية والولايات المتحدة الأمريكية ظلت لفترة طويلة مرتعاً خصباً للإجرام الإلكتروني، بل إن هذه الدول بما حققته من تقدم علمى وتكنولوجى كانت أحد الأسباب الرئيسية لانتشار الجريمة الإلكترونية في ربوع العالم.

ومن الأهمية بمكان اعتبار أن جرائم الكمبيوتر والحاسبات الإلكترونية، هي ظاهرة إجرامية جديدة ومستجدة تعطى إنذارات لكل مستخدمي هذا الجهاز بالخطر، بغية تنبيه مجتمعات العصر الراهن بشأن كم الكوارث والخسائر التي تخلفها الجرائم المعلوماتية والرقمية؛ فجريمة الحاسب الآلي جريمة رقمية تتمتع بتقنيات عالية وليست مرئية، ينفذها محترفون في الأجرام الرقمى، يمتلكون أدوات المعرفة التقنية للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة.

وتأسيساً على ما سبق، فإن هذه الدراسة تتناول قضايا ثورة المعلومات من الناحية الضارة للبشر والإنسانية، وهو الجزء الخاص بالجرائم والاعتداء على حقوق الغير. ورغم ذلك لا تبدو قوانين العقوبات المحلية في حالتها الواهنة العاجزة عن ملاحقة التطور العلمي، مؤهلة للتعامل مع مثل هذا النمط الجديد من الجرائم، الأمر الذى يحتم ضرورة التفكير جدياً في مراجعة قوانين العقوبات الوطنية وتطويعها بالشكل الذى يناسب ويلائم لغة العصر.

إن وسائل الاتصال لم تخترع الجريمة، بل كانت ضحية لها في معظم الأحوال، حيث أن هذه الوسائل تعرضت لسوء الاستغلال من قبل كثيرين، ومن الثابت أيضاً أن المجرمين وظفوا الاتصال تاريخياً لخدمة النشاطات الإجرامية التي يقومون بها. أما الجريمة فهي ذاتها الجريمة في قديم التاريخ، وحديثه، لا يختلف على بشاعتها، وخطرها على المجتمع الإنساني أحد، ولذلك اتفق على مواجهتها، ومن أجلها أقيمت المحاكم، وسُنّت العقوبات.

ومن المؤكد أن المجرم المعلوماتي والجريمة المعلوماتية تختلف عن مرتكبي الأفعال الإجرامية التقليدية، لذا من الطبيعي أن نجد الاختلاف نفسه في الأسباب والعوامل التي تدفع في ارتكاب الفعل غير المشروع، فضلاً عن ذلك، تتمتع جرائم الكمبيوتر والمعلوماتية بعدد من الخصائص التي تختلف تماماً عن

الخصائص التي تتمتع بها الجرائم التقليدية، كما أن الجانى الإلكتروني يختلف أيضاً عن المجرم العادي.

وتمثل غاية التعلم إحدى أهم بواعث الجريمة المعلوماتية، حيث تقوم على استخدام الكمبيوتر والإمكانيات المستحدثة لنظم المعلومات، وما يرتبط بها من طموحات الربح والمكاسب وإن هناك من يعتدي على نظم المعلومات دون وجه حق، وفقاً لدوافع شخصية ومؤثرات خارجية، وهذا قد يكون مدعاةً للإقدام على تنفيذ الجريمة المعلوماتية أو إحدى جرائم الإنترنت.

وتسعى الحكومة المصرية جاهدةً من أجل جذب الاستثمارات في مجال التكنولوجيا، إلا ان هناك فراغاً تشريعياً في هذا المجال خصوصاً في قضايا النشر الإلكتروني وقوانين جرائم الإنترنت الخاصة باقتحام النظم وغيرها، فلا يوجد في مصر نظام قانوني خاص بجرائم المعلومات، إلا أن القانون المصري يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعاً من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكونة لأركان الجريمة المعلوماتية.

واالواقع يحتم على الجميع التكاتف من أجل مواجهة الجرائم المعلوماتية، وفق آليات مؤسسية وتشريعية مدروسة وواعية، للخروج من هذا النفق المظلم وتفعيل الآليات الموجوده على أرض الواقع سواء كانت حكومية او خاصة، المهم أن يتم التخلص أو حتى تحجيم جرائم العالم الافتراضي التي باتت أكثر ضرراً وفتكاً من جرائم الواقع.

وتقع الدول العربية في مهبّ الجرائم الإلكترونية، ذلك أن هذه الجرائم لم تترك بلداً من بلاد العالم إلا واخترقتها ونالت من أهداف محددةٍ فيها، بما في ذلك الدول العربية.

ومن الضرورى أن يتم تدشين قواعد قانونية حديثة للمجتمع المعلوماتى

ضمن قانون الإجراءات الجنائية من أجل وضع معلومات معينة تحت تصرف السلطة المهيمنة على التحقيق في مجال جرائم الإنترنت والمعلوماتية؛ ويرجع ذلك لأن المجرمين من محترفى انتهاك شبكات الحاسبات الآلية ومرتكبى الجرائم ذات الصلة، يقومون بتخزين معلوماتهم في أنظمة تقنية المعلومات وعلى نحو متطور، وتصطدم الأجهزة المكلفة بالتحقيق بهذا التكنيك لتخزين المعلومات وهي التي تسعى للحصول على أدلة الإثبات.

ونظراً لسهولة حركة المعلومات في مجال أنظمة تقنية المعلومات حيث تجعل هذه السهولة لحركة المعلومات أنه بالإمكان ارتكاب جريمة عن طريق حاسب آلي موجود في دولة معينة، بينما يتحقق نتيجة هذا الفعل الإجرامي في دولة أخرى، وهو الأمر الذي استلزم ضرورة وجود تعاون دولي محكم في مجال مكافحة هذا النوع من الجرائم ولأجل توفير حماية حقيقية لأنظمة الاتصالات.

# قائمة مراجع الكتاب


**أ ـ الكتب :**

**الأستاذ/ أحمد أمين :**

ـ شرح قانون العقوبات الأصلى ـ القسم الخاص1923 .

**د . أحمد فتحى سرور :**

ـ الوسيط في قانون العقوبات، القسم الخاص ـ 1979 .

**د . أحمد محمد محرز :**

ـ القانون التجارى، 1986/ 1987 .

**د . أكثم أمين الخولى :**

ـ الأموال التجارية، مطبعة نهضة مصر بالفجالة ـ القاهرة 1964 .

ـ الوسيط في الأعمال التجارية ـ القاهرة 1964 .

**د . أبو اليزيد علي المتيت :**

ـ الحقوق على المصنفات الأدبية والفنية والعلمية، منشأة دار المعارف، الإسكندرية، الطبعة الأولى 1967 .

**آمنة علي يوسف:**

- قراصنة أنظمة الكمبيوتر، المؤتمر القومى الثالث عشر لأمن الكمبيوتر، ديسمبر 1998.

**انتصار. نوري الغريب.**

- أمن الكمبيوتر والقانون، دار الراتب العالمية، لبنان، 1994.

**د. إبراهيم أحمد الصعيدي وآخرون:**

- الحاسب الإلكتروني ونظم المعلومات الإدارية، موسوعة دلتا كمبيوتر، مطابع المكتب المصري الحديث، 1993.

**د. علاء الدين محمد مصطفى وآخرون:**

- الموسوعة الشاملة لمصطلحات الحاسب الإلكترونى، موسوعة دلتا كمبيوتر، مطابع الكتاب المصري، عالم الجداول الالكترونية، دائرة معارف الحاسب الإلكترونى.

**د. محمد زكي عبد المجيد وآخرون:**

- فيروسات الحاسب وأمن البيانات، موسوعة دلتا كمبيوتر ووسائل حمايتها، دار النهضة العربية، عام 1989.

**د. محمد فهمي طلبه وآخرون:**

- الحاسبات الإلكترونية حاضرها ومستقبلها، موسوعة دلتا للكمبيوتر، مطابع الكتاب المصري الحديث 1992.
- الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، القاهرة 1991. مطابع المكتب المصري الحديث.

**د. هاني كمال مهدي وآخرون:**

- المرجع الشامل لنظام التشغيل DES موسوعة دلتا كمبيوتر1991.

**د. حسام الدين كامل الأهوائي:**

- أصول القانون، بدون ناشر، 1988.

**د. حسن صادق المرصفاوي:**

- جرائم المال، سنة 1956.

**د. سميحة القليوبي:**

- القانون التجارى، دار النهضة العربية، طبعة عام 75/ 1976.
- الوجيز في التشريعات الصناعية، القاهرة، 1967.

**د. رؤوف عبيد:**

- جرائم الاعتداء على الأشخاص، دار الفكر العربي، 1985.
- جرائم الاعتداء على الأشخاص والأموال، الطبعة السابعة، 1978.

**د. عبد الحميد الجمال:**

- مبادئ القانون الكتاب الثاني، العلاقات القانونية، الفتح للطباعة والنشر، الإسكندرية، 1990.

**د. عبد الرزاق السنهوري:**

- الوسيط في شرح القانون المدنى، القاهرة 1968.

**د. عبد العظيم مرسي وزير:**

- شرح قانون العقوبات ـ القسم الخاص ـ جرائم الاعتداء على الأموال، دار النهضة العربية 1993.

**د. عبد الفتاح الصيفي:**

- قانون العقوبات اللبنانى ـ جرائم الاعتداء على أمن الدولة وعلى الأموال، دار النهضة العربية، بيروت 1972.

**د. عبد المهيمن بكر:**

- القسم الخاص في قانون العقوبات، الطبعة السابعة 1977.

**د. عمر السعيد رمضان:**

- شرح قانون العقوبات، القسم الخاص، دار النهضة العربية 1975.

**د. عوض محمد:**

- جرائم الأشخاص والأموال، دار المطبوعات الجامعية، الإسكندرية.
- قانون الإجراءات الجنائية، الجزء الأول، 1989، مؤسسة الثقافة.

**د. فوزية عبد الستار:**

- شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، 1983.

**د. محسن شفيق:**

- القانون التجاري، القاهرة، 1949.

**د. محمد زكي:**

- الإثبات في المواد الجنائية، بدون ناشر، ص16.

**د. محمد محيي الدين عوض:**

- القانون الجنائي، جرائمه الخاصة 1978/ 1979.
- قانون العقوبات السوداني.

**د. محمد مختار بربري:**

- قانون المعاملات التجارية، دار الفكر العربي، سنة 1987.

**د. محمود محمود مصطفى:**

- القسم الخاص، دار النهضة العربية، الطبعة الثامنة 1984.

**د. محمود مصطفى القللي:**

- شرح قانون العقوبات في جرائم الأموال، الطبعة الأولى، 1939.

**د. محمود نجيب حسنى:**

- جرائم الاعتداء على الأموال في قانون العقوبات اللبنانى، دار النهضة العربية، بيروت 1969.
- شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، 1988.
- دروس في قانون العقوبات، القسم الخاص، دار النهضة العربية 1970.

**مصطفى الجمال:**

- مبادئ القانون، الكتاب الثاني، العلاقات القانونية، الفتح للطباعة والنشر، الإسكندرية، 1990.

**د. ماجد عمار:**

- المسئولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها، دار النهضة العربية، 1989، ص35.

**د. محمد حسام لطفي:**

- الحماية القانونية لبرامج الحاسب الآلي، دار الثقافة للطباعة والنشر. القاهرة 1987.

**د. محمد حسني عباس:**

- الملكية الصناعية والمحل التجاري، القاهرة، 1977.

**د. محمد سامي الشوا:**

- ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، الطبعة الثانية 1998.

**د. محمد محي الدين عوض:**

ـ مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات ـ القاهرة 1993.

**د. نبيل إبراهيم سعد:**

ـ المدخل إلى القانون الكتاب الثاني، نظرية الحق، دار النهضة العربية، بيروت 1995.

**د. يسر أنور ود. آمال عثمان:**

ـ شرح قانون العقوبات، القسم الخاص، الجزء الأول 1975.

**د. جلال أحمد خليل**

ـ النظام القانوني لحماية الاختراعات ونقل التكنولوجيا إلى الدول النامية، جامعة الكويت، 1992.

**د. جميل عبد الباقي الصغير:**

ـ القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناتجة عن استخدام الحاسب الآلي، الطبعة الأولى، دار النهضة العربية، 1992.

ـ الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دار النهضة العربية، 1990.

**د. طارق سرور:**

ـ كلية الحقوق جامعة القاهرة، ذاتية جرائم الإعلام الإلكتروني (دراسة مقارنة) الطبعة الأولى ـ دار النهضة النهضة العربية، 2011.

**د. عمر الفاروق الحسيني:**

ـ المشكلات العامة في جرائم الحاسب الآلي وأبعادها الدولية، دراسة

تحليلية نقدية بنصوص التشريع المصري مقارنا بالتشريع الفرنسى، الطبعة الثانية، 1994 .

**د. غانم محمد غانم:**

- عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مؤتمر القانون والكمبيوتر والإنترنت ـ الإمارات، مايو 2000.

**د. هاني دويدار:**

- نطاق احتكار المعرفة التكنولوجية بواسطة السرية، دار الجامعة الجديدة، 1996 .

**د. هدى حامد قشقوش:**

- جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية 1992.

**د. هشام محمد فريد رستم:**

- قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة أسيوط 1994 .

**د. هلالي عبد اللاه أحمد:**

- تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، طبعة، 1997 دار النهضة العربية .

**د. برهام محمد عطا الله:**

- المصنفات المحمية في قانون حماية حق المؤلف، منشور في كتاب حق المؤلف بين الواقع والقانون، مركز البحوث والدراسات القانونية، كلية الحقوق جامعة القاهرة، 1990 .

**مركز البحوث والدراسات بشرطة دبي ـ الإمارات العربية المتحدة:**

ـ بحث بعنوان: جرائم الكمبيوتر، 1998، دار النهضة العربية، منشورات 1993.

**ب ـ الرسائل العلمية:**

**د. خالد حمدي عبد الرحمن:**

ـ الحماية القانونية للكيانات المنطقية، رسالة دكتوراة، حقوق عين شمس 1992.

**د. عبد القدوس عبد الرازق محمد:**

ـ التأمين من المسئولية وتطبيقاته الإجبارية المعاصرة، دراسة مقارنة بين قانون المعاملات المدنية لدولة الإمارات العربية المتحدة وبين القانون المصري» رسالة دكتوراة، جامعة القاهرة، سنة 1999.

**د. عزة محمود أحمد خليل:**

ـ مشكلات المسئولية المدنية في مواجهة فيروس الحاسب. رسالة دكتوراة مقدمة إلى حقوق القاهرة، عام 1994.

**د. عمرو ابراهيم الوقاد:**

ـ النظرية العامة للاختلاس في جرائم المال الخاص. رسالة دكتوراة، حقوق عين شمس.

**د. محمد محمد عنب:**

ـ معاينة مسرح الجريمة، رسالة دكتوراة، أكاديمية الشرطة، كلية الدراسات العليا القاهرة 1988.

**د. يونس خالد عرب مصطفى:**

ـ جرائم الحاسوب دراسة مقارنة، رسالة ماجستير، الجامعة الأردنية، 1994.

**ج ـ الدوريات**

**د. أحمد فتحي سرور:**

ـ نظرية الاختلاس، التشريع المصرى، مجلة إدارة قضايا الحكومة، 1969.

**د ـ المؤتمرات**

**د. أسامة محمد محي الدين عوض:**

ـ جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات. بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 1993.

**د. هدى حامد قشقوش:**

ـ بحث مقدم للجمعية المصرية للقانون الجنائى 1993، بعنوان: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات.

**د. زكي أمين حسونة:**

ـ جرائم الكمبيوتر والجرائم الأخرى في مجال التكتيك المعلوماتي، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 1993.

**العقيد/ علاء الدين محمد شحاته:**

ـ رؤية أمنية للجرائم الناشئة عن استخدام الحاسب الآلي ـ بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 1993.

**د. محمد الأمين البشري:**

ـ التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت ـ جامعة الإمارات العربية المتحدة، سنة 2000.

**هـ ـ صحف**

**جريدة البيان:**

ـ العدد7537 ـ 2001، العدد 7633 ـ 2001.

**تقرير اتحاد منتجي برامج الكمبيوتر.**

ـ العدد 7661 ـ 1997 دبي ـ الإمارات العربية المتحدة.

**جريدة الخليج:**

ـ العدد 6658.

**صفحة أخبار الدار:**

ـ 1997 العدد 7989 ـ 2001 ـ الشارقة ـ الإمارات العربية المتحدة.

# الفهرس

## المستشار/ أيــمـن رســــلان في ســطور

**الرئـيس بمحكمة الإسـتئناف وأمـن الدولـة العليـا بالقـاهـرة**

**وحاليا القاضي بمحاكم دبي بدولة الإمارات العربية المتحدة**

- مواليد 16/ 10/ 1969 بالقاهرة.
- حاصل على ليسانس الحقوق وبكالوريوس العلوم الشرطية من كلية الشرطة المصرية بالقاهرة بتقدير عام جيد جداً عام 1991.
- عمل ضابط شرطة بالأمن العام وبالإدارة العامة للمرور بجمهورية مصر العربية منذ تخرجه عام 1991 وحتى عام 1994.
- تم تعيينة بالنيابة العامة من عام 1994 حتى عام 2000 ثم قاضياً بمحاكم مصر.
- فى عام 2004 تم انتدابة عضواً بالمكتب الفنى للإدارة العامة للخبراء والطب الشرعى بديوان عام وزارة العدل مع إلحاقة لبعض الوقت للمكتب الفنى لمعالى وزير العدل..
- تم ترقيتة لدرجة مستشار بالإستئناف العالي عام 2010 وتعيينة مستشاراً بمحكمة الجنايات وأمن الدولة العليا حتى ترقّى الى درجة رئيس محكمة الاستئناف.
- تم تعيينة وكيلاً لإدارة محاكم مصر بديوان عام وزارة العدل ومديراً لإدارة المأذونين والموثقين المنتدبين بوزارة العدل المصرية.
- تم انتدابة رئيساً وعضواً بكثير من اللجان الوزارية أبرزها عضواً باللجنة الرئيسية لتنسيق مقرات المحاكمات الكبرى فى مصر ومنها محاكمة القرن.
- قام بوضع مشروع قانون المأذونين والموثقين المنتدبين بوزارة العدل المصرية بمفردة تمهيداً لتقديمة للجنة المختصة كخطوة أولى لعرضة على البرلمان المصري.

- قام بالمشاركة في الكثير من المؤتمرات الدوليه ممثلاً لوزارة العدل المصرية ومحاكم مصر .
- قام بإلقاء الكثير من المحاضرات القانونية فى مختلف المراكز والمعاهد القضائية والقانونية بالقاهرة.
- له مؤلف بمركز البحوث الجنائية بالقاهرة بعنوان الجذور التاريخية للإرهاب والذي حصل على عدة جوائز.
- فى نهاية عام 2012 تم إعارته قاضياً بمحاكم دبى بدولة الإمارات العربية المتحدة.
- عمل قاضياً بمحاكم دبي وحصل على شهادات تقدير لجهودة المتميزة فى تحقيق أعلى معدلات الإنجاز للقضايا العمالية.
- حصل على جائزة القاضي الإلكتروني لمحاكم دبي فى ديسمبر 2013.
- تم تكريمة من رئاسة المحكمة العمالية فى ذات العام، كما تم تكريمه من الادارة العامه لشرطة دبي.
- تم تعيينة بالإضافة لعملة بمحاكم دبي بقرار من سمو الشيخ حاكم دبي قاضياً بمركز فض المنازعات الإيجارية ببلدية دبي بأول دفعة قضاة عند إنشاء المركز.
- قام بإلقاء محاضرات حول قانون العمل الاماراتي بنادي شرطة دبي ومعهد دبي القضائي وآخرها محاضرات فى برنامج دبلوم مكافحة جرائم الاتجار بالبشر بدولة الامارات العربيه المتحدة.